مراقبة المراقبين: حماية حقوق الإنسان في عصر الرقابة الجماعية

ملخص

"الحقيقة المرة هي أن استخدام تقانة الرقابة الجماعية إنما تعصف فعلياً بالحق في خصوصية الاتصالات على شبكة الانترنت كلياً" .

بن إميرسون، مستشار الملكة، **المقرر الخاص للأمم المتحدة المعني بتعزيز وحماية حقوق الإنسان** في سياق مكافحة الإرهاب.

في 5 يونيو/حزيران 2013 نشرت صحيفة "ذي غارديان" البريطانية أولى حلقات التسريبات المتعلقة بالرقابة الجماعية العشوائية من قبل وكالة الأمن الوطني في الولايات المتحدة وقيادة الاتصالات الحكومية في المملكة المتحدة. وقد قدم إدوارد سنودن، كاشف التجاوزات الذي كان قد عمل مع وكالة الأمن الوطني، أدلة ملموسة على وجود برامج رقابة عالمية على الاتصالات للتنصت على الاتصالات عبر الانترنت والهواتف لمئات الملايين من الأشخاص في شتى أنحاء العالم.

ربما يكون لدى الحكومات أسباب مشروعة لمراقبة الاتصالات، من قبيل مكافحة الجريمة أو حماية الأمن القومي. بيد أنه نظراً لأن الرقابة تشكل انتهاكاً للحق في الخصوصية وحرية التعبير، فإن اللجوء إليها يجب أن يلتزم بمعايير صارمة: إذ يجب أن تكون الرقابة مستهدفة، وأن تستند إلى اشتباه معقول، وأن تتم وفقاً للقانون، وأن تكون ضرورية لتلبية هدف مشروع، وبطريقة تتناسب مع الهدف ولا تنطوي على تمييز. وهذا يعني أن الرقابة الجماعية التي تهدف إلى جمع اتصالات أعداد ضخمة من الناس بصورة عشوائية عمل لا يمكن تبريره. كما أنها تشكل انتهاكاً للحق في الخصوصية والحق في حرية التعبير.

ويقدم هذا التقرير الموجز لمحة عامة عن المعلومات التي كُشف عنها النقاب في السنتين الماضيين بشأن برامج عمليات الرقابة الجماعية التي تديرها حكومتا الولايات المتحدة والمملكة المتحدة وغيرهما من الحكومات، فضلاً عن التطورات القانونية والسياسية والتقنية الرئيسية المتعلقة بالرقابة الجماعية وبالحق في الخصوصية خلال تلك الفترة، وفي هذا التقرير الموجز تقدم منظمة العفو الدولية ومنظمة الخصوصية الدولية خطة عمل من أربع نقاط لضمان حماية حقوق الإنسان في العصر الرقمي.

وفي السنتين الماضيتين عرفنا حجم برامج الرقابة الجماعية التي تديرها بشكل رئيسي وكالة الأمن الوطني وقيادة الاتصالات الحكومية بتعاون وثيق مع شقيقاتهما في أستراليا وكندا ونيوزيلندا – والمعروفة معاً باسم "حلف العيون الخمس" (أو العيون الخمس). إن التسريبات التي فضحتها وسائل الإعلام بناء على الملفات التي سرَّبها إدوارد سنودن تضمنت أدلة على ما يلي:

– أُرغمت الشركات – ومنها فيس بوك وغوغل وميكروسوفت – على تسليم بيانات زبائنها بموجب أوامر سرية من خلال برنامج "بريزم" التابع لوكالة الأمن الوطني؛

– قامت وكالة الأمن الوطني بتسجيل وتخزين وتحليل البيانات المتعلقة بكل مكالمة هاتفية ورسالة نصية بُثت في المكسيك وكينيا والفلبين؛

– اختارت وكالة الأمن الوطني وقيادة الاتصالات الحكومية بعض أضخم شركات الاتصالات السلكية واللاسلكية لاعتراض الكوابل البحرية عبر المحيط الأطلسي والتنصت على الاتصالات الخاصة التي تنقلها من خلال برنامجيْ "تيمبورا" TEMPORA و"أبستريم" Upstream؛

– قامت قيادة الاتصالات الحكومية البريطانية ووكالة الأمن الوطني الأمريكية بقرصنة شبكة الحاسوب الداخلي لشركة "غيمالتو"، وهي المصنِّع الأكبر لبطاقات "سيم SIM" في العالم، ربما لسرقة مليارات مفاتيح التشفير المستخدمة لحماية خصوصية الاتصالات عبر الهواتف الخليوية حول العالم.

وقد تزايدت المعارضة الشعبية في شتى بلدان العالم. إذ أظهر استطلاع للرأي نظمته منظمة العفو الدولية، حيث سألت 15,000 شخص من 13 بلداً في جميع القارات، أن 71 بالمئة من الناس يعارضون بشدة قيام حكوماتهم بالتجسس على اتصالاتهم عبر الانترنت والهواتف.

وأعربت مؤسسات دولية وإقليمية، وكذلك خبراء دوليون وإقليميون، من قبيل المفوض السامي للأمم المتحدة لحقوق الإنسان والجمعية البرلمانية لمجلس أوروبا، عن قلق كبير بشأن برامج الرقابة الجماعية، وحذرت من الخطر الذي تشكله هذه البرامج على حقوق الإنسان. وفي ديسمبر/كانون الأول 2014 اعتمدت الجمعية العامة للأمم المتحدة قراراً ثانياً حول الحق في الخصوصية في العصر الرقمي، حيث أعربت عن قلقها العميق من التأثير السلبي الذي قد تُحدثه مراقبة و/أو التنصت على الاتصالات، ولاسيما عندما يتم ذلك على نطاق جماعي، على ممارسة حقوق الإنسان والتمتع بها." وفي مارس/آذار 2015، أنشأ مجلس حقوق الإنسان في الأمم المتحدة للمرة الأولى نطاق صلاحيات دائم لمقرر خاص معني بالحق في الخصوصية، وهو ما يعدُّ خطوة تاريخية من شأنها ضمان وضع قضايا الخصوصية في مقدمة جدول أعمال الأمم المتحدة في السنوات القادمة.

وقد قضت المحاكم في عدد من البلدان ضد المراقبة الجماعية وتبادل المعلومات الاستخبارية. ففي المملكة المتحدة قَضت محكمة سلطات التحقيق بأنه، قبل الأحكام التي أصدرتها المحكمة في ديسمبر/كانون الأول 2014 وفبراير/شباط 2015، شكَّل النظام الذي يحكم عمليات التماس وتلقِّي وتخزين وبث الاتصالات الخاصة بالأشخاص الموجودين في المملكة المتحدة من قبل السلطات البريطانية، والتي حصلت عليها السلطات الأمريكية من خلال برنامجيْ "بريزم" و"أبستريم"، مخالفةً للاتفاقية الأوروبية لحقوق الإنسان. وفي الولايات المتحدة، قضت محكمة استئناف فدرالية في مايو/أيار 2015 بأن الحصول على تسجيلات الهواتف في الولايات المتحدة كان عملاً غير قانوني.

كما تجرَّأ العديد من أضخم شركات التكنولوجيا في العالم على رفع أصواتها ضد الرقابة الجماعية. ففي عام 2013 أطلقت عشر شركات – من بينها أبل وفيس بوك وغوغل وميكروسوفت وتويتر وياهو – الائتلاف العالمي لإصلاح نظام الرقابة الحكومية، الذي يدعو، من جملة إصلاحات قانونية أخرى، إلى وضع حد لممارسات جمع المعلومات الجماعية بموجب "قانون الوطنية" الأمريكي.

واتخذت عدة شركات كبرى خطوات ملموسة أكثر ضد الرقابة ب عن طريق زيادة درجة الأمن والتشفير المقدَّمة إلى المستخدمين عبر برامجها وخدماتها، وتوفير حماية أفضل لخصوصية مستخدمي الانترنت من الرقابة الجماعية العشوائية.

كما أن ثمة علامات على وجود إصلاحات قانونية محدودة. فعلى سبيل المثال، فإن قانون الحرية في **الولايات المتحدة الأمريكية**، الذي أقره مجلس النواب في مايو/أيار، يحاول وضع حد لعمليات الجمع الجماعية لتسجيلات الهواتف[1] في الولايات المتحدة من قبل الحكومة. بيد أن القانون يطلب من الشركات حجب بيانات معينة والبحث عنها وتحليلها بناء على طلب الحكومة، الأمر الذي يوسِّع الأساس القانوني لجمع البيانات على نطاق واسع بدلاً من وضع حد له. وبالإضافة إلى ذلك، لا تزال هناك جوانب أخرى عديدة للرقابة الأمريكية غير مقنَّنة ولا تخضع للمساءلة بموجب القانون الجديد — بما في ذلك الرقابة الجماعية المفروضة على ملايين الأشخاص خارج الولايات المتحدة. وثمة حاجة إلى ممارسة الضغط لضمان قيام الحكومات بتفكيك أنظمة الرقابة المتفشية بشكل استثنائي في الداخل والخارج. ولعل الخطوة الأولى في هذا الاتجاه تتمثل في الاعتراف بأن الحقوق المتعلقة بالخصوصية إنما هي حقوق مملوكة على نحو متساو للأشخاص الذين يعيشون في داخل البلد المعني وفي خارجه على حد سواء.

وعلى عاتق الشركات تقع مسؤولية احترام الحق في الخصوصية على الانترنت. وللإيفاء بهذه المسؤولية، يتعين عليها اتخاذ خطوات أكثر جرأة بكثير لزيادة الأمن على برامجها وخدماتها، كي لا تصبح بيانات المستخدمين الخاصين لقمة سائغة في متناول أيدي الحكومات.

وثمة تيار صاعد للآراء المناهضة للرقابة الجماعية، ولكن الكثير ما زال على المحك. وقد سنَّت حكومات خارج إطار "حلف العيون الخمس" قوانين جديدة منحتها سلطات رقابة جماعية. وشهد هذا العام صلاحيات رقابة جديدة كاسحة في باكستان وفرنسا، في الوقت الذي تستعد فيه الدنمرك وسويسرا وهولندا والمملكة المتحدة لتقديم مشاريع قوانين بشأن المعلومات الاستخبارية في المستقبل القريب.

إن المحافظة على الخصوصية، وبالتالي على حرية التعبير، أمر يقتضي عملاً منسقاً من قبل الأفراد والفنيين والخبراء القانونيين ومنظمات المجتمع المدني والمنظمات الدولية والشركات والحكومات. ولا يوجد حل كاف بمفرده؛ بل ثمة حاجة إلى مزيج من الإصلاحات القانونية المحلية والمعايير الدولية القوية وتقنيات الحماية المتطورة للخصوصية والتزام الشركات بخصوصية المستخدم، كما أن ثمة حاجة إلى العمل الفردي.

الرقابة الجماعية على الاتصالات عبر الانترنت والهواتف: ما عرفناه بشأن برامج الولايات المتحدة والمملكة المتحدة

لقد بتنا نعلم، عن طريق تسريبات سنودن، أن وكالات الاستخبارات الأمريكية والبريطانية ما فتئت تدير برامج رقابة جماعية عشوائية على نطاق عالمي، مكَّنتهما من اعتراض جزء كبير من حركة الاتصالات عبر الانترنت، بالإضافة إلى الاتصالات عبر الهاتف لمئات الملايين من سكان الكرة الأرضية. وقد اقترنت هذه القدرات بحجم ضخم من تبادل المعلومات الاستخبارية بين الدول الأعضاء في "حلف العيون الخمس"، فضلاً عن شبكة من وكالات المخابرات في عشرات البلدان حول العالم.[2] وفيما يلي بعض البرامج التي تديرها وكالة الأمن الوطني وقيادة الاتصالات الحكومية، التي كشف عنها النقاب منذ عام 2013.

ملحوظة بشأن المعلومات المتعلقة بممارسات الرقابة من قبل الولايات المتحدة والمملكة المتحدة: إن الأغلبية العظمى من المعلومات المتعلقة بممارسات الرقابة الجماعية من قبل الولايات المتحدة والمملكة المتحدة في الفضاء العام تستند إلى وثائق سرَّبها كاشف التجاوزات والمحلل السابق في وكالة الأمن الوطني إدوارد سنودن. وتضم الوثائق المسرَّبة وثائق داخلية لوكالة الأمن الوطني وقيادة الاتصالات الحكومية. كما أن بعض التسريبات يتضمن معلومات حول أنشطة رقابية من قبل بلدان أخرى. وقد نُشرت التسريبات المتعلقة بممارسات الرقابة الجماعية من قبل العديد من الوكالات الصحفية في بلدان عدة.

وأكدت حكومة الولايات المتحدة وجود بعض البرامج التي فضحتها التسريبات، من قبيل برنامج "بريزم". بيد أنه لم يتم تأكيد أو نفي المعلومات الواردة في معظم التسريبات من قبل الحكومتين الأمريكية والبريطانية. وفي غياب رفض الولايات المتحدة أو المملكة المتحدة للمعلومات الواردة في تلك التسريبات، ونظراً لأن صدقية الوثائق التي سرَّبها سنودن لم تكن موضع طعن من قبل أي من البلدين، فإن المعلومات المتعلقة ببرامج الرقابة يُفترض أن تكون صحيحة.

1. اعتراض شبكات الاتصالات السلكية واللاسلكية العالمية

تقوم وكالة الأمن الوطني وقيادة الاتصالات الحكومية بالتنصت المباشر على الكوابل البحرية للإنترنت عبر المحيط الأطلسي عن طريق برنامجي "أبستريم" و"تيمبورا" على التوالي.[3] ويتنصت هذان البرنامجان على كميات ضخمة من الاتصالات على الانترنت، حيث تُجرى عمليات مسح ضوئي وفلترة لكل اتصال يمر عبر الكوابل التي تشكل العمود الفقري للإنترنت. إن اعتراض الكابل البحري يمدُّ وكالات الاستخبارات البريطانية والأمريكية بسلطات مراقبة غير مسبوقة.

ففي فترة دامت ستة أشهر، قامت قيادة الاتصالات الحكومية بموجب برنامج "أوبتك نيرف"، بالتنصت على 1.8 مليون محادثة بالفيديو عبر "ياهو"، والتقطت صور ضمَّت بين 3 – 11 بالمئة من "صور التعري غير المرغوب فيها" قبل معالجتها بواسطة تقانة التعرف على الوجوه.[4]

وفي كندا تقوم مؤسسة أمن الاتصالات الكندية بالتنصت على الكوابل وتسجيل ما يصل إلى 15 مليون عملية تنزيل يومياً من مواقع تبادل الملفات، من قبيل "رابيد شير"Rapidshare أو "ميغوبلود" Megaupload.[5] كما تقوم المؤسسة بمراقبة مئات الرسائل الإلكترونية وتخزينها "لأيام أو أشهر" مع تطبيق تقانة التحليل.[6]

وفي نيوزيلندا يستخدم مكتب أمن الاتصالات الحكومي التنصت عبر الأقمار الاصطناعية لالتقاط بيانات الانترنت والهاتف التي تُبث إلى منطقة آسيا والمحيط الهادئ ومنها. وفي عام 2009 قام المكتب بتطوير القاعدة الرئيسية في وايهوباي لتصبح "ذات طاقة استيعابية كاملة"، بما يضمن القدرة على التقاط كافة الاتصالات التي تمر عبر شبكاته، وتبادل البيانات الخام مع "حلف العيون الخمس".[7]

2. الوصول إلى مراكز البيانات والأنظمة الداخلية للشركات

أُرغمت تسع شركات، من بينها أبيل وفيس بوك وغوغل وميكروسوفت وياهو على تسليم بيانات زبائنها بموجب أوامر سرية صدرت كجزء من برنامج "بريزم" التابع لوكالة الأمن الوطني،[8] ومُنعت من الحديث عنها علناً.[9]

ثم تآمرت وكالة الأمن الوطني وقيادة الاتصالات الحكومية لاقتحام روابط الاتصالات الرئيسية التي تربط مراكز البيانات لبعض هذه الشركات حول العالم. وبموجب هذا البرنامج، الذي أطلق عليه الاسم الرمزي (مسكولار) فإن ملايين التسجيلات تُلتقط في كل يوم من موقع ياهو الداخلي وشبكات غوغل.[10]

وفي تلك الأثناء استهدفت قيادة الاتصالات الحكومية شركة "بلجاكوم"، وهي المزوِّد الأكبر للاتصالات السلكية واللاسلكية في بلجيكا. وقرصنت الوكالة البريطانية حواسيب الموظفين الداخلية كي تتمكن من التقاط الاتصالات الخاصة التي تجريها الشركة. ولدى شركة بلجاكوم ملايين الزبائن، ومن بينهم مسؤولون من المفوضية الأوروبية والبرلمان الأوروبي ومجلس أوروبا.[11]

3. تعقُّب مواقع هواتفنا الخليوية

تقوم وكالة الأمن الوطني بجمع نحو خمسة ملايين تسجيل يومياً تتعلق بأماكن وجود الهواتف الخليوية حول العالم، باستخدام مجموعة من البرامج المعروفة باسم "كو-ترافيلار". ووفقاً لتقرير موجز لوكالة الأمن الوطني، فإن المنظمة تقوم بجمع الكثير من المعلومات المتعلقة بالمواقع بموجب البرنامج، إلى حد أن الإمكانات "تتجاوز قدرتنا على إدخال البيانات ومعالجتها وتخزينها".[12]

4. التنصُّت على المكالمات الهاتفية في بلد بأسره

لقد حصلت وكالة الأمن الوطني على نسخ من كل مكالمة هاتفية في البلاد بأسرها. ويُشار إلى برنامج التنصت الصوتي، الذي يُطلق عليه اسم رمزي هو "ميستيك" و"سومالغيت" على أنه "آلة الزمن" لأنه يمكِّن وكالة الأمن الوطني من إعادة تشغيل التسجيلات في أي هاتف بدون أن يكون هناك شخص مستهدف بالمراقبة مسبقاً.[13] وقد استُخدم أصلاً لتسجيل جميع المكالمات الصوتية في جزر البهاما وأفغانستان، والتقاط البيانات التفصيلية لجميع المكالمات الصوتية في كل من المكسيك وكينيا والفلبين، والأمر الذي يطال عدد سكان يتجاوز 250 مليون نسمة.

5. كسب التأييد لقوانين الرقابة في الخارج

ثمة فريق في وكالة الأمن الوطني معروف باسم قسم الشؤون الخارجية يهدف إلى الضغط على البلدان الأخرى أو حفزها على تغيير قوانينها بحيث تسمح بفرض الرقابة الجماعية والتعاون مع الوكالة.[14] ويبحث هذا الفريق عن ثغرات في القوانين وأشكال الحماية الدستورية التي من شأنها أن تمكّن الوكالات الأجنبية الشريكة من القيام بعمليات الرقابة الجماعية، التي لم تتصورها الهيئة التشريعية.

وقال إدوارد سنودن إن كلاً من السويد وألمانيا وهولندا "تلقت تعليمات من وكالة الأمن الوطني، أحياناً تحت ستار وزارة الدفاع الأمريكية وغيرها من الهيئات، حول كيفية تخفيض مستوى الحماية القانونية لاتصالات بلدانها".[15]

كما تقدم قيادة الاتصالات الحكومية إرشادات مشابهة: إذ تقول إحدى وثائقها: "إن لدى الهولنديين بعض القضايا التشريعية، التي ينبغي أن يعملوا من خلالها، قبل أن تسمح لهم البيئة القانونية بالعمل بالطريقة التي تعمل بها قيادة الاتصالات الحكومية. إننا نقدم مشورة قانونية بشأن كيفية تناول بعض تلك القضايا مع المحامين الهولنديين." [16]

6. نشر الرقابة الجماعية

من أجل الحصول على مزيد من المعلومات من حلفائها في ما وراء البحار، تقوم "العيون الخمس" بتزويدهم بالمعدات والخبرات لمساعدة الأجهزة الشريكة في اعتراض الكوابل البحرية في مناطقها.[17] وتساعد التكنولوجيا أولئك الشركاء على "إدخال" كميات هائلة من البيانات بطريقة تسهّل معالجتها وتوفر نسخة من الاتصالات التي يتم التنصت عليها إلى "العيون الخمس". ففي عام 2011، أنفقت وكالة الأمن الوطني 9 مليون دولار أمريكي على برامج الوصول إلى الكوابل الأجنبية، حيث يعمل حالياً أكثر من 13 موقعاً فيما وراء البحار، اثنان منها في ألمانيا والدنمرك.[18] وفي ألمانيا تقوم وكالة Bundesnachrichtendienst (بي إن دي) بالتنصت على الاتصالات عبر الأقمار الاصطناعية والكوابل، وذُكر أنها تشاطر 220 مليون تسجيل هاتفي يومياً مع وكالة الأمن القومي.[19]

7. تقويض معايير التشفير

ما انفكت وكالة الأمن القومي وقيادة الاتصالات الحكومية تعمدان إلى تخريب معايير التشفير، وتعملان على إضعاف القدرة على الاتصال الآمن عن طريق برنامجيين لفك التشفير، وهما "بولرن" Bullrun (وكالة الأمن الوطني) و"إيجهل" Edgehill (قيادة الاتصالات الحكومية).

في عام 2010 أوضحت وثيقة من وثائق قيادة الاتصالات الحكومية أن "وكالة الأمن الوطني قادت، على مدى العشرية الماضية، جهوداً عدائية ومتعددة الأوجه لكسر تقنيات التشفير المستخدمة على نطاق واسع على الانترنت"، وإدخال عناصر ضعف في أنظمة التشفير التجارية".[20] وفي الوقت نفسه كُشف النقاب عن أن وكالة الاتصالات الحكومية كانت تقوم باستكشاف طرق لاقتحام البيانات المشفَّرة في فيس بوك وغوغل وهوت ميل وياهو على ميكروسوفت.[21] وأنشأت وكالة الاتصالات الحكومية فريق عمليات الاستخبارات البشرية (هيومنت)، وهذا الفريق "مسؤول عن تحديد وتجنيد وإدارة عملاء سريين في صناعة الاتصالات السلكية واللاسلكية العالمية،[22] بحسب وثيقة داخلية للوكالة.

8. قرصنة الهواتف والتطبيقات

قام "حلف العيون الخمس" ببناء قدراته في مجال إصابة الأجهزة الفردية بعدوى برمجيات خبيثة بغرض التمكُّن من "استغلال أي هاتف في أي مكان في أي وقت"[23] على حد تعبيره. وقد تبجَّح الجواسيس البريطانيون والأمريكيون بأن المعلومات "إذا كانت موجودة على الهاتف فإننا نستطيع الحصول عليها".[24] وبدلاً من استخدام هذا التكتيك في الظروف الاستثنائية فقط، فقد طوَّر "حلف العيون الخمس" تلك الأدوات لإصابة ملايين الحواسيب والهواتف في سائر أنحاء العالم.[25] بل إن مؤسسة أمن الاتصالات الكندية تجسست على الحواسيب والهواتف الذكية التي تتصل بوزارة التعدين والطاقة البرازيلية بهدف جمع معلومات استخبارية اقتصادية.[26] وفي عرض تسرَّب من وكالة الأمن الوطني، علَّقت الوكالة على قدراتها الخاصة بالقول: "مَن كان يعرف في عام 1984 أن [الهاتف الذكي] سيكون بمثابة "الشقيق الأكبر" وأن "الزومبي" سيكونون الزبائن الذين يدفعون الثمن؟"[27]

9. التحكم بالبنية التحتية الأساسية للاتصالات

إن وكالة الأمن الوطني، التي تعمل في شراكة مع شركات الاتصالات السلكية واللاسلكية، منخرطة في تشكيل "حركة المرور" "بشكل عدائي" بهدف تغيير مسار الاتصالات عبر الانترنت على نحو مصطنع وإعادة توجيهها بحيث تمر في نقاط التنصت التابعة "للعيون الخمس".[28] وعندما تفشل في ذلك، تعمد "العيون الخمس" إلى استخدام البرمجيات الخبيثة سراً في شبكات الاتصالات السلكية واللاسلكية كي تتمكن من نسخ "حركة المرور" في بنيتها التحتية للرقابة الجماعية. وتتمثل إحدى الطرق التي تستخدمها وكالة الأمن الوطني لتحقيق ذلك في "اعتراض" شحنات "هاردوير" الحواسيب عند تسليمها إلى الزبائن وتغييرها لضمان قدرتها على الوصول إلى الشبكات "حول العالم".[29]

وفي الجوهر، بالإضافة إلى اعتراض الاتصالات التي تعبر حدود بلديهما فإن وكالة الأمن الوطني وقيادة الاتصالات الحكومية تحاولان إعادة توجيه حركة مرور الاتصالات بحيث تمر عبر محابسها، بما يسمح بالتنصت عليها وجمعها وتحليلها. وبهذه الطريقة يتم اختيار البنية التحتية الأساسية للإنترنت لتلقيم البيانات في برامج المراقبة التابع "لحلف العيون الخمس".

10. سرقة مفاتيح التشفير

قامت قيادة الاتصالات الحكومية ووكالة الأمن الوطني بقرصنة شبكة الحاسوب الداخلية لشركة "غيمالتو"، وهي المصنِّع الأكبر لبطاقات SIM في العالم، وسرقت ملايين مفاتيح التشفير المستخدمة لحماية خصوصية اتصالات الهواتف الخليوية حول العالم.[30] وباستخدام مفاتيح التشفير المسروقة هذه، تستطيع وكالات الاستخبارات فتح اتصالات الهواتف الخليوية بدون حاجة إلى الحصول على موافقة من شركات الاتصالات، وتجنب الحاجة إلى الحصول على إذن، مع عدم ترك أية آثار على الشبكة اللاسلكية للمزوِّد تدل على أنه تم التنصت على الاتصالات.

[الرأي العام العالمي يرفض الرقابة الجماعية]

أظهر استطلاع رأي دولي أجرته منظمة العفو الدولية على 15,000 من المستطلع آرائهم من 13 بلداً من سائر قارات العالم، أن 71% مما استطلع آراءهم يعارضون بشدة قيام حكومات بلدانهم بالتجسس على اتصالاتهم عبر الانترنت والهاتف. وقد أُجري الاستطلاع في فبراير/شباط 2015.

النتائج الرئيسية للاستطلاع:

فيما يتعلق بالرقابة من قبل حكومات بلدانهم:

- في البلدان الثلاثة عشر جميعاً التي شملها الاستطلاع، رفض المستطلَعة آراؤهم قيام حكومات بلدانهم بالتنصت على اتصالاتهم عبر الانترنت والهواتف وتخزينها وتحليلها. وبالمتوسط، بلغت نسبة الأشخاص الذين عارضوا الرقابة من قبل حكوماتهم (59%) ضعف نسبة الذين وافقوا على الرقابة (26%).
- إن أغلبية الذين عارضوا الرقابة الجماعية من قبل حكومات بلدانهم هم من البرازيل (65%) وألمانيا (69%) وأسبانيا (67%)، حيث قوبلت الأنباء التي أفادت بأن وكالة الأمن الوطني تنصَّتت على 60 مليون مكالمة هاتفية إسبانية بالغضب في عام 2013، قد تصدَّرت طاولة المعارضة أيضاً.
- إن أغلبية المواطنين الأمريكيين (63%) وقفوا ضد خطة حكوماتهم المتعلقة بالرقابة الحكومية، مقارنةً بنحو 20% فقط وقفوا معها.

فيما يتعلق بالرقابة الجماعية من قبل الولايات المتحدة على البلدان الأخرى

- 71% مما استطلع آراءهم عارضوا بشدة قيام الولايات المتحدة بمراقبة استخدامهم للإنترنت.
- المعارضة الأشد لقيام الولايات المتحدة بالتنصت على اتصالات الانترنت وتخزينها وتحليلها جاءت من ألمانيا (81%)، ثم البرازيل (80%).
- حتى في البلد الأقل معارضة (فرنسا)، فإن الأغلبية لا تزال تعارض قيام الولايات المتحدة بعمليات المراقبة الجماعية (56%).
- وفي كل من استراليا وكندا ونيوزيلندا والمملكة المتحدة – وهي البلدان التي تشاطرها الولايات المتحدة ثمار الرقابة الجماعية – بلغت نسبة المعارضين للرقابة من قبل الولايات المتحدة (70%)، أي ثلاثة أضعاف نسبة المؤيدين (17%).

فيما يتعلق بدور الشركات

- يعتقد 60% من الأشخاص أن على عاتق شركات التقانة يقع واجب مساعدتهم على تأمين معلوماتهم الشخصية من تدخل الحكومات، بينما وافق 26% منهم فقط على السماح للحكومات بالوصول إلى البيانات.

الخبراء والهيئات الدولية يعتبرون الرقابة الجماعية انتهاكاً لحقوق الإنسان

على مدى العامين المنصرمين أعلن عدد من الخبراء والهيئات الدولية والإقليمية والوطنية البارزة أن الرقابة الجماعية تشكل انتهاكاً لحقوق الإنسان. وهؤلاء معاً يشكلون رأياً عاماً ذا صدقية ضد اشكال الرقابة الجماعية من قبيل تلك التي تمارسها وكالة الأمن الوطني وقيادة الاتصالات الحكومية.

ففي ديسمبر/كانون الأول 2013 جاء أولاً تقرير **المجلس الاستشاري للرئيس**، وهو مجلس خبراء عقده الرئيس باراك أوباما للتدقيق في تسريبات سنودن. وقد أدان المجلس برامج الرقابة الجماعية لوكالة الأمن الوطني، وقال: "إنه يجب ألا يُسمح للحكومة بجمع وتخزين كافة المعلومات الجماعية الشخصية وغير العامة وغير الناضجة المتعلقة بالأفراد بهدف الاستفسارات وتحليل البيانات في المستقبل لأغراض الحصول على معلومات استخبارية أجنبية".[31]

ووجد رأي المجلس صدى له في قرار صدر في الشهر نفسه عن **الجمعية العامة للأمم المتحدة**، أعربت فيه عن القلق العميق بشأن التأثير السلبي الذي يمكن أن يُحدثه التنصت على بيانات الاتصالات وجمعها على التمتع بحقوق الإنسان،[32] ولاسيما عندما يتم ذلك على نطاق جماعي واسع.

في يناير/كانون الثاني 2014، **وجد مجلس مراقبة الخصوصية والحريات المدنية**، وهو وكالة مستقلة داخل حكومة الولايات المتحدة، أن جمع الكم الأكبر من تحليل بيانات الهواتف من قبل وكالة الأمن الوطني غير مسموح به بموجب الفصل 215 من قانون الوطنية للولايات المتحدة الأمريكية. كما أعلن التقرير أن ذلك يشكل انتهاكاً لقانون خصوصية الاتصالات الإلكترونية، وأثار بواعث قلق بشأن التعديلين الأول والرابع.[33]

وفي فبراير/شباط 2014 قدمت لجنة البرلمان الأوروبي المعنية بالحريات والعدالة والشؤون الداخلية للتحقيق في برامج الرقابة التي تستخدمها وكالة الأمن الوطني تقريرها، الذي أظهر أن "مكافحة الإرهاب لا يمكن أن تكون مبرراً لوضع برامج رقابة جماعية غير مستهدفة أو سرية أو حتى غير قانونية".[34] و"تتبنى اللجنة الرأي القائل إن مثل هذه البرامج لا تتسق مع مبدأيْ الضرورة والتناسب في المجتمع الديمقراطي."

في يوليو/تموز 2014، وفي تقرير بعنوان "الحق في الخصوصية في العصر الرقمي"، أعلنت **المفوضة السامية للأمم المتحدة لحقوق الإنسان**، أن مجرد وجود برنامج مراقبة جماعية... إنما يخلق نوعاً من التدخل في الخصوصية".[35]

وفي أكتوبر/تشرين الأول 2014 تعززت النتائج التي توصلت إليها المفوضة السامية بموقف **المقرر الخاص للأمم المتحدة المعني بتعزيز حقوق الإنسان في سياق مكافحة الإرهاب**، الذي أدان الرقابة الجماعية حيث قال: "إن الحقيقة المرة هي أن استخدام تقانة الرقابة الجماعية يقضي من الناحية الفعلية على الحق في خصوصية الاتصالات عبر الانترنت جملة وتفصيلاً."[36]

وتضمَّن قرار ثانٍ **للجمعية العامة للأمم المتحدة**، صدر في ديسمبر/كانون الأول 2014، تكراراً للمشاعر التي تضمَّنها قرار عام 2013، حيث أعرب عن قلق الدول العميق من "التأثير السلبي الذي قد تُحدثه الرقابة أو/و التنصت على الاتصالات...، ولاسيما عندما يتم ذلك على نطاق جماعي واسع، على ممارسة حقوق الإنسان والتمتع بها."[37]

كما أدلى **مفوض مجلس أوروبا لحقوق الإنسان** بدلوه، حيث كتب ورقة بعنوان: حكم *القانون على الانترنت وفي العالم الرقمي الأوسع*، قال فيها: لقد أصبح من الواضح على نحو متزايد أن برامج الرقابة السرية الهائلة والعشوائية لا

تتماشى مع القانون الأوروبي لحقوق الإنسان، ولا يمكن تبريرها بمكافحة الإرهاب أو غيره من الأخطار الكبرى التي تهدد الأمن القومي".[38]

في أبريل/نيسان 2015 اعتمدت **الجمعية البرلمانية لمجلس أوروبا** قراراً خاصاً، تضمَّن تنديداً بالرقابة، ربما يكون الأكثر صراحةً حتى الآن. وذكر القرار "أن الممارسات الرقابية التي كُشف عنها النقاب حتى الآن تُعرِّض حقوق الإنسان الأساسية للخطر، ومن بينها الحق في الخصوصية وحرية المعلومات والتعبير، والحق في المحاكمة العادلة وحرية المعتقد. ولاسيما عندما يتم التنصت على اتصالات المحامين ورجال الدين والتلاعب بالأدلة الرقمية. إن هذه الحقوق هي بمثابة حجر الزاوية للديمقراطية، وإن تعريضها للخطر بدون رقابة قضائية كافية تؤدي إلى تعريض حكم القانون للخطر."[39]

وأخيراً– وهو الأكثر أهمية– نشير إلى أن **مجلس حقوق الإنسان التابع للأمم المتحدة** اتخذ خطوة حاسمة عندما اعتمد بالإجماع قراراً في مارس/آذار 2015، أُنشأت بموجبه آلية خبير مستقل دائم معني بالحق في الخصوصية.[40] وسيتم تعيين المقرر الخاص المعني بالخصوصية في جلسة يونيو/حزيران 2015 للمجلس، وستشمل مسؤولياته إعداد تقارير حول الانتهاكات المزعومة للحق في الخصوصية، ومنها تلك التي تنشأ "بالارتباط بالتحديات التي تخلقها التقنيات الجديدة".[41]

التدقيق القضائي لممارسات الرقابة الجماعية حول العالم

منذ يونيو/حزيران 2013 بدأت منظمات المجتمع المدني والشركات والمحامون بتقديم عدد من الطعون القانونية ضد الرقابة الجماعية في جميع بلدان "العيون الخمس"، إلى جانب بلدان أخرى يُعتقد أن لديها برامج رقابة جماعية موسعة. ويجدر بالذكر أن أحكاماً صدرت في المملكة المتحدة والولايات المتحدة وجدت أن بعض ممارسات قيادة الاتصالات الحكومية ووكالة الأمن الوطني غير قانوني. وثمة قضايا مهمة عديدة معلقة في المحاكم الوطنية والمحكمة الأوروبية لحقوق الإنسان.

العيون الخمس

ما هو "حلف العيون الخمس"؟[42]

"حلف العيون الخمس" هو ترتيب عالمي لعمليات رقابة سرية بين دول يضم وكالة الأمن الوطني في الولايات المتحدة وقيادة الاتصالات الحكومية في المملكة المتحدة، ومؤسسة أمن الاتصالات في كندا، ومديرية الإشارات الدفاعية في استراليا ومكتب أمن الاتصالات الحكومية في نيوزيلندا.

وقد بدأ الحلف في عام 1949، ويهدف إلى تبادل المعلومات الاستخبارية وبشكل أساسي مخابرات الإشارات SIGINT. وبموجب اتفاقية الحلف، تُدار عمليات التنصت على المعلومات وجمعها والحصول عليها وتحليلها وفك شيفرتها من قبل كل واحدة من الدول الأطراف في الجزء الخاص بها من الكرة الأرضية، ويتم تبادل كافة المعلومات الاستخبارية بشكل مفروغ منه. لأن هذه الاتفاقية واسعة النطاق، وتُنشيء مراكز عمليات تُدار بشكل مشترك، حيث يعمل عناصر من وكالات الاستخبارات المتعددة لدول العيون الخمس جنباً إلى جنب.

ففي **المملكة المتحدة**، وفي عام 2013، قدمت منظمة الخصوصية الدولية ومنظمة العفو الدولية وثماني منظمات أخرى لحقوق الإنسان دعوى قانونية ضد ممارسات الرقابة على الاتصالات في المملكة المتحدة. ونتيجةً لذلك قضت محكمة سلطات التحقيق في فبراير/شباط 2015 بأن تبادل المعلومات الاستخبارية بين الولايات المتحدة والمملكة المتحدة كان عملاً غير قانوني قبل صدور الأحكام في ديسمبر/كانون الأول 2014 وفبراير/شباط 2015 لأن القواعد التي تنظم وصول المملكة المتحدة إلى برنامجي "بريزم" و"أبستريم" كانت سرية.[43]

وخلال سير الإجراءات القانونية، اضطرت حكومة المملكة المتحدة على الإفصاح عن المعلومات بشأن العلاقة مع الولايات المتحدة في تبادل المعلومات الاستخبارية. وفي الوقت الذي اعتبرت فيه المحكمة أن المملكة المتحدة أصبحت، بعد الإفصاح عن تلك المعلومات، ملتزمة بالمادة 8 (الحق في الخصوصية) من الاتفاقية الأوروبية، فإن المنظمات المدعية لم توافق على ذلك، ورفعت القضية إلى المحكمة الأوروبية لحقوق الإنسان. وثمة قضيتان أخريان مرفوعتان ضد ممارسات الرقابة من قبل المملكة المتحدة لم يتم البتُّ فيهما بعد أمام المحكمة الأوروبية لحقوق الإنسان. والمدعون في القضية هم منظمة مراقبة الشقيق الأكبر، ومنظمة "بن" الإنجليزية PEN، ومجموعة الحقوق المفتوحة، ومكتب الصحافة الاستقصائية.[44]

وفي المحكمة الأوروبية لحقوق الإنسان كذلك، طعنت منظمة الخصوصية الدولية بتاريخ... في الإعفاء الشامل من قوانين حرية المعلومات الممنوح لوكالة الاستخبارات البريطانية (قيادة الاتصالات الحكومية). وقد مُنعت منظمة الخصوصية الدولية من الوصول إلى اتفاقية العيون الخمس، والوثائق التي تنظم عمل حلف التجسس السري. وتم تأجيل الطعن المقدم إلى المحكمة، والذي اعتبر أن الإعفاء الشامل يشكل انتهاكاً للحق في تلقي وإرسال المعلومات، المنصوص عليه في المادة 10 من الاتفاقية الأوروبية لحقوق الإنسان، إلى (التاريخ...) بانتظار صدور القرار في قضية أخرى.[45]

وبالإضافة إلى ذلك، طعن سبعة مزوِّدين لخدمات الانترنت والاتصالات في كل من المملكة المتحدة والولايات المتحدة وألمانيا وهولندا وكوريا الجنوبية وزمبابوي في استخدام القرصنة وأساليب استغلال شبكة الحاسوب من قبل قيادة الاتصالات الحكومية. وعند رفع الدعوى القانونية حثَّ المدعون حكومة المملكة المتحدة على إبراز مسودة مدونة لقواعد الممارسات بشأن "تدخل المعدات"، وهو ما يعتبر بحد ذاته انتصاراً إذا أخذنا بعين الاعتبار أنه لم يتم تأكيد استخدام القرصنة من قبل أجهزة الاستخبارات البريطانية رسمياً من قَبل. وستُعقد جلسة الاستماع للقضية من قبل محكمة سلطات التحقيق في عام 2015.[46]

وفي الآونة الأخيرة، وتحديداً في مايو/أيار 2015، أصدرت **محكمة الاستئناف في الدائرة الثانية بالولايات المتحدة** حكماً لصالح الاتحاد الأمريكي للحريات المدنية، حيث وجدت أن عمليات جمع تسجيلات الهواتف بشكل جماعي لم يكن مسموحاً بها في الفصل 215 من قانون الوطنية.[47] وقالت المحكمة إن "التطوير الواسع لمخزونات الحكومة للتسجيلات الخاصة السابقة سيمثل تقليصاً غير مسبوق لتوقعات جميع الأمريكيين المتعلقة بالخصوصية". ولم يكن مسموحاً به في التشريعات على ما يبدو.[48] وأضافت المحكمة تقول: إن مثل هذا الزخم في التدخل في الخصوصية ينبغي أن "يسبقه حوار حقيقي، وأن يعبَّر عنه بلغة لا يعتريها الخطأ".[49]

في **كندا** قدم مجلس الحريات المدنية في كولومبيا البريطانية دعوى قانونية ضد وكالات المخابرات الإلكترونية الكندية – مؤسسة أمن الاتصالات الكندية – ادعى فيها أن الرقابة السرية والمنفلتة من عقالها على الكنديين عمل غير دستوري.[50] ويُذكر أن الدعوى لا تزال قائمة.

في **نيوزيلندا** قدم حزب الخضر شكوى إلى المفتش العام للمخابرات والأمن بشأن مزاعم قيام جهاز الرقابة، وهو مكتب أمن الاتصالات الحكومية، بالتجسس على النيوزيلنديين في المحيط الهادئ. وفي مارس/آذار 2015 أعلن المفتش العام للمخابرات والأمن أنه سيبدأ تحقيقاً، ليس في مزاعم محددة فحسب، وإنما في جميع الاجراءات وأنظمة الالتزام لدى مكتب أمن الاتصالات الحكومية.[51]

كما طُلب من المفتش العام للمخابرات والأمن في **أستراليا** إجراء تحقيق في أفعال مديرية الإشارات الدفاعية الأسترالية ودورها في عملية الرقابة الجماعية التي تقوم بها "العيون الخمس"، ولكنه رفض المضي قدماً في هذا التحقيق.

التحديات في بلدان أخرى

في **هولندا** طعن ائتلاف من المواطنين ومنظمات المجتمع المدني في ممارسات تبادل المعلومات الاستخبارية لجهاز المخابرات العامة والأمن الهولندي وجهاز المخابرات العسكرية والأمن الهولندي. وفي قضية مرفوعة أمام محكمة المقاطعة في لاهاي، قال المدعون إن عملية تلقي واستخدام المعلومات الاستخبارية الأجنبية عن طريق برامج الرقابة الجماعية الأمريكية يجب أن تتوقف.[52] بيد أن المحكمة رفضت الطلب. وستقوم الحكومة الهولندية في هذا العام بإجراء مراجعة شاملة لقانون الرقابة.

وفي **ألمانيا**، قال طعن قانوني قدمه المحامي نيكو هارتنغ ضد جهاز المخابرات الفدرالي (بي إن دي) إن "الرقابة الاستراتيجية" للرسائل الإلكترونية الأجنبية أمر غير دستوري. وقد رُفضت القضية لأسباب إجرائية – إذ وجدت المحكمة أن السيد هارتنغ لا يملك الحق القانوني في تقديم الدعوى.

مَن هم الذين تم التجسس عليهم؟

تُبرر الحكومات ممارسة الرقابة الجماعية بذريعة الأمن القومي بشكل دائم تقريباً. بيد أن سنودن كشف النقاب عن أن قدراتها وبرامجها تُستخدم في نهاية المطاف في سياقات تتجاوز ما هو ضروري لحماية الأمن القومي. فبالإضافة إلى التنصت على اتصالات مئات الملايين من الناس العاديين، فقد وضعت وكالة الأمن الوطني وقيادة الاتصالات الحكومية جماعات محددة وأفراد معينين على "لائحة المراقبة" والتجسس عليهم. ومن بين أولئك المستهدفين:

منظمة أطباء العالم[53]

وهي منظمة دولية معروفة تماماً ومحترمة للغاية، تقدم الرعاية الطبية إلى "المتضررين من الحرب أو الكوارث الطبيعية أو المرض أو الجوع أو الفقر أو الإقصاء".[54]

"لقد صُدمنا بالمزاعم التي وصلت إلى حد التبديد المخجل لأموال دافعي الضرائب؛ وهي أموال يُستحسن أن تُنفق على توفير اللقاحات ضد الشلل للأطفال السوريين، أو إعادة بناء النظام الصحي المدمَّر في الفلبين، أو في أي مكان آخر من العالم كان بحاجة ماسة إليها في ذلك الوقت."

ليه دينز، المدير التنفيذي لمنظمة أطباء العالم في المملكة المتحدة.[55]

خواكين ألمونيا، نائب رئيس المفوضية الأوروبية

كُشف النقاب عن أن وكالة الأمن الوطني وقيادة الاتصالات الحكومية تجسستا على خواكين ألمونيا، نائب رئيس المفوضية الأوروبية المكلف بالإشراف على سياسة المنافسة. وتركز صلاحياته على "النضال ضد الكارتيلات ومنع الشركات المهيمنة من إساءة استخدام قوتها في السوق في أي قطاع أو أي بلد بأوروبا، والتدقيق الصارم في عمليات دمج الشركات المقترحة".[56]

"إن (ما ورد في التسريبات) أمر غير مقبول ويستحق منا الشجب بأشد العبارات. فهذا ليس نوع السلوك الذي نتوقعه من شركاء استراتيجيين، ناهيك عن الدول الأعضاء."

بيا أهرينكيلد، الناطق الرسمي بلسان المفوضية الأوروبية.

منظمة الأمم المتحدة للطفولة (يونيسف)[57]

"يونيسف" هي وكالة الأمم المتحدة التي تضطلع بتعزيز حقوق الأطفال ورفاههم على الصعيد العالمي. وتقوم المنظمة بدعم تعليم الفتيات وتعمل في مجال تحصين الأطفال وتغذيتهم ومنع انتشار فيروس نقص المناعة المكتسب/مرض الأيدز في صفوف الشباب.[58]

أحمد موفق زيدان، مدير مكتب قناة الجزيرة في باكستان [59]

وضعت وكالة الأمن الوطني أحمد موفق زيدان، وهو صحفي استقصائي محترم ومدير مكتب الجزيرة في إسلام أباد منذ فترة طويلة، على "لائحة مراقبة الإرهاب" بناء على تحليل بيانات جمعتها الوكالة.

" بالنسبة لنا نحن الصحفيين، كي نستطيع تقديم معلومات للعالم، ينبغي توفير إمكانية الاتصال بحرية بالشخصيات ذات الصلة في المجال العام، والتحدث إلى أشخاص على الأرض، وجمع معلومات حرجة... والقول أنني، أو أي صحفي آخر، عضو في أية جماعة استناداً إلى دفتر اتصالاته أو سجل مكالماته الهاتفية أو مصادره إنما يعتبر تشويهاً للحقيقة وانتهاكاً كاملاً لمهنة الصحافة." أحمد موفق زيدان، الجزيرة.

فيصل جيل [60]

تبيَّن أن فيصل جيل، وهو عضو في الحزب الجمهوري الأمريكي، ويحمل تصريح أمني "سري للغاية"، وعمل في وزارة الأمن الوطني في ظل الرئيس جورج بوش، هو أحد الشخصيات المسلمة العامة في الولايات المتحدة الذين وُضعوا على قائمة المستهدفين بالمراقبة من قبل وكالة الأمن الوطني ومكتب التحقيقات الفدرالي.

"لا أدري لماذا .. فقد فعلت كل ما بوسعي في حياتي كي أكون وطنياً. خدمتُ في سلاح البحرية وفي الحكومة، وكنت ناشطاً في مجتمعي المحلي – فعلت كل ما ينبغي على مواطن صالح أن يفعله برأيي."
فيصل جيل

سعي الحكومات إلى التمتع بسلطات رقابية أكبر

على الرغم من المعارضة الجدية فإن حكومات "العيون الخمس" لم تتخذ أية خطوات تُذكر في سبيل تفكيك برامج الرقابة الجماعية في السنتين الماضيتين. وفي حالة المملكة المتحدة سعت الحكومة إلى تسويغ وتوسيع الممارسات غير القانونية الموجودة. وفي بلدان أخرى سنَّت الحكومات قوانين جديدة، منحت بموجبها لنفسها سلطات رقابة جماعية. وفي بعض الحالات ربما مثَّلت هذه القوانين الجديدة محاولة لوضع أساس قانوني للرقابة غير القانونية التي كانت تمارسها الحكومات أصلاً.

ففي يوليو/تموز 2014، مرّرت حكومة **المملكة المتحدة** على عجل قانوناً جديداً، وهو قانون الاحتفاظ بالبيانات وسلطات التحقيق باعتباره "مشروع قانون طارئ"، وأقرّه البرلمان في يوم واحد. وقد صُمم القانون لمراجعة قانون الاحتفاظ بالبيانات في المملكة المتحدة رداً على قرار الحكم الذي أصدرته محكمة العدل الأوروبية في أبريل/نيسان 2014، الذي أبطل مفعول التوجيه الخاص بالاحتفاظ بالبيانات لعام 2009. ولا ينص القانون على الاحتفاظ المستمر والشامل ببيانات الاتصالات، الأمر الذي يتناقض بشكل مباشر مع حكم محكمة العدل الأوروبية، فحسب، وإنما يوسِّع نطاق سلطات التنصت البريطانية من خلال السماح للحكومة بمطالبة الشركات المتمركزة خارج المملكة المتحدة بالالتزام بالمذكرات الصادرة عن الحكومة.[61]

وبالإضافة إلى ذلك، فإن مشروع قانون بيانات الاتصالات أو ما يُعرف باسم "ميثاق سنوبرز"، يُحتمل أن يعود إلى المملكة المتحدة عقب انتخابات حكومة أغلبية من المحافظين في مايو/أيار 2015. ومن شأن هذا التشريع المثير للجدل، الذي هُزم بصعوبة في عام 2014، والذي قوبل بمعارضة واسعة من جماعات الدفاع عن الخصوصية وحقوق الإنسان، أن يوسِّع نطاق صلاحيات المخابرات البريطانية، وأن يسمح بالوصول إلى معظم بيانات الاتصالات من قبل أجهزة أخرى داخل المملكة المتحدة، كجهاز الشرطة مثلاً.

وفي الولايات المتحدة، وعلى النقيض من ذلك، اتُّخذت خطوات محدودة للحد من عمليات الرقابة الجماعية. فقد رد الرئيس أوباما على تسريبات سنودن بإصدار توجيه رئاسي ينحو إلى رسم حدود للاحتفاظ بالبيانات التي جُمعت وتوزيعها.[62] وعلاوةً على ذلك، فقد ناقش الكونغرس قضية إصلاح الرقابة، وأقرَّ مجلس النواب قانون الحرية، الذي يحاول وضع حد لقيام الحكومة بجمع تسجيلات الهواتف بشكل جماعي.[63] بيد أن القانون يطلب من الشركات حجب بيانات

معينة والبحث عنها وتحليلها بناء على طلب الحكومة، مما يوسِّع الأساس القانوني لعملية جمع البيانات على نطاق واسع بدلاً من وضع حد لها. كما سعى الكونغرس إلى توسيع نطاق وصول وكالة الأمن الوطني إلى المعلومات الشخصية باسم تعزيز الأمن الإلكتروني.

وعلاوةً على ذلك، فإن العديد من الجوانب الأخرى لعمليات الرقابة الأمريكية لا تزال غير مقننة وغير قابلة للمساءلة بموجب القانون الجديد – بما في ذلك فرض الرقابة الجماعية على ملايين الأشخاص خارج الولايات المتحدة. وإضافة إلى ذلك، فإن القانون لا يكبح بشكل كاف عمليات التنصت وجمع المعلومات الأخرى، غير تسجيلات الهواتف، ولا يكفل الإشراف الحقيقي عليها من قبل المحكمة الخاصة بمراقبة المعلومات الاستخبارية الأجنبية.

إن الخطر الذي يتهدد الخصوصية، وبالتالي حرية التعبير، قد ازداد كذلك لأن بلداناً خارج إطار "حلف العيون الخمس" حاولت قوننة سلطات رقابية أقوى. فقد شهد هذا العام اقتراح إضافة سلطات رقابية جديدة كاسحة في التشريعات في كل من باكستان وفرنسا وسويسرا، في الوقت الذي يُتوقع سنُّ مشروع قانون جديد يتعلق بالمعلومات الاستخبارية في هولندا في المستقبل القريب.

في أبريل/نيسان 2015 وافق المجلس الوطني **الباكستاني** على مشروع قانون جديد بشأن الجرائم الإلكترونية، نصّ على توسيع سلطات الرقابة الحكومية بشكل مفرط. وهذا القانون المسمى "قانون منع الجرائم الإلكترونية" هو حالياً بانتظار التصويت عليه في مجلس الشيوخ. وفي حالة الموافقة عليه، فإنه سيسمح لمزودي الخدمة بالاحتفاظ بالبيانات المتعلقة باتصالات المواطنين الهاتفية وبالبريد الإلكتروني لمدة لا تقل عن سنة.[64] وبالإضافة إلى ذلك، فإن مشروع القانون سيسمح للحكومة الفدرالية بتبادل المعلومات الاستخبارية التي يتم جمعها عن طريق التحقيقات مع وكالات استخبارية أجنبية، ومن بينها وكالة الأمن الوطني، بدون الحاجة إلى إذن قضائي. ويتضمن مشروع القانون صلاحيات واسعة وغير محددة بشكل كاف "بالاستيلاء" على البيانات (المشار إليه في مشروع القانون بعبارة "الحصول على نسخة من البيانات"، ولكنه لا يحدد الإجراءات التي ينبغي اتباعها للقيام بذلك. وبترك هذا الأمر لتقدير الحكومة الفدرالية، فإن القانون لا يقدم قواعد واضحة يمكن الحصول عليها بسهولة بما يتماشى مع للقانون الدولي لحقوق الإنسان.

في فرنسا، وفي مايو/أيار 2015 سنَّ مجلس النواب في البرلمان قانوناً جديداً خاصاً بالمعلومات الاستخبارية يتضمن سلطات رقابية كاسحة. ويسمح مشروع القانون، الذي تقول عنه الحكومة إنه يمثل أداة ضرورية لمنع الإرهاب (بدون تعريف هذا المصطلح في القانون) لرئيس الوزراء باتخاذ تدابير رقابية لأغراض أخرى عديدة وغير محددة من قبيل "الدفاع عن المصالح الأساسية للسياسة الخارجية"، ومنع "أي شكل من أشكال التدخل الأجنبي". إن محتوى هذه المصطلحات الغامضة غير واضح، وإن ثمة قلقاً من أن تُستخدم لأسباب غالباً ما لا يكون لها علاقة بمنع الأفعال الخاطئة. أما الأمر الأكثر إثارة للجدل فهو أن مشروع القانون يتجاهل حاجة وكالات المخابرات إلى طلب إذن أو الحصول عليه من القضاء.

ولذا فإن القانون يتجاهل بشكل أساسي متطلبات الإشراف والمساءلة التي يجب أن تخضع لها وكالات المخابرات الفرنسية، في الوقت الذي يمنحها سلطات أوسع وأكثر تدخلاً. فعلى سبيل المثال، فإن مشروع القانون، ولغايات منع الإرهاب، يشترط على مزودي الانترنت والاتصالات السلكية واللاسلكية وضع "صناديق سوداء" في البنية التحتية لتسجيل تحليلات البيانات؛ كما يسمح للعملاء الأمنيين بقرصنة أجهزة الحاسوب والهاتف الخليوي، واقتفاء أثر مواقع الأشخاص والتجسس على البريد الإلكتروني والنصوص وغيرها من الاتصالات لشخص يعتقدون أنه ربما يكون على صلة بشخص آخر متورط في أنشطة مشبوهة، حتى لو كان ذلك بغير قصد، أو لأنهما موجودان في المنطقة الجغرافية نفسها، وذلك باستخدام جهاز يُعرف باسم *IMSI Catcher* للتنصت على وفك شيفرة الرسائل النصية القصيرة والمكالمات الهاتفية من جميع الهواتف الخليوية ضمن دائرة قطرها مئات الأمتار.

ولعل أكثر الجوانب إثارة للقلق في مشروع القانون هذا هو ما لا يقوله المشروع، وبشكل خاص تلك الثغرة الكبرى التي يتضمنها، والتي يمكن أن تمهِّد الطريق إلى ممارسة الرقابة الجماعية العشوائية على كافة أشكال استخدامات الانترنت. وبالفعل فإن مشروع القانون يبيح لرئيس الوزراء السماح بالتنصت على الاتصالات "المرسلة إلى أو الواردة من الخارج. ولا يُذكر شيء عن أساليب الرقابة التي يمكن استخدامها بخصوص هذه الاتصالات، وبدلاً من ذلك ستُذكر هذه الأساليب في مرسوم سري، وبذلك يتم تجاوز البرلمان. وعلاوةً على ذلك، فإن مشروع القانون لا يقول شيئاً بأية طريقة ذات معنى عن الشروط المطلوبة لتنفيذ مثل هذه الرقابة، وماهية الإجراءات التي يتعين على السلطات اتّباعها. هذه هي المثالب الحاسمة بشكل خاص في التشريع المقترح، آخذين بعين الاعتبار أن حجماً ضخماً من الاتصالات على الانترنت يُنقل عبر خوادم موجودة خارج البلاد. إن مثل هذا الصمت في مشروع القرار يمهِّد الطريق لاستخدام الرقابة التعسفية والعشوائية ضد المواطنين الفرنسيين وغير الفرنسيين.

وفي سويسرا تجري حالياً مراجعة مشروعي قرارين يعطيان السلطات السويسرية صلاحيات رقابية جديدة واسعة. إذ أن مشروع قانون الاستخبارات يمنح أجهزة المخابرات سلطات التنصت على الاتصالات التي تمر عبر كوابل الانترنت التي تعبر **سويسرا**. أما مشروع القانون الثاني فإنه يتضمن شرطاً يقضي باحتفاظ مزودي الاتصالات السلكية واللاسلكية بالبيانات الخاصة بكافة الاتصالات لمدة 12 شهراً.

ويبدو أن بلداناً أوروبية أخرى تحذو حذوها. ففي **هولندا** تقترح الحكومة تحديث قانون أجهزة المخابرات والأمن بُغية استغلال "النمو الهائل في شبكات الكوابل الدولية" بحسب توصية "لجنة ديسنز في ديسمبر/كانون الأول 2013.[65] وفي ردها الرسمي على اللجنة، اقترحت الحكومة الهولندية خططاً للسماح بعملاء المخابرات بالوصول إلى كوابل الانترنت التي تمر عبر هولندا (شبيهة كثيراً ببرنامجي "أبستريم" في الولايات المتحدة و"تيمبورا" في المملكة المتحدة).[66] ومن شأن ذلك أن يمهِّد الطريقة لممارسة التنصت العشوائي وجمع وتخزين مواد الاتصالات السلكية واللاسلكية التي لا تستهدف فرداً أو مجموعة أو موقعاً محدديْن ومميَّزين، ولا تستند إلى اشتباه معقول. إن الحكومة الهولندية تستعد لتقديم مشروع قانونها الجديد بشأن التنصت الجماعي في غضون الأشهر القليلة القادمة.

كما تتنامى الضغوط السياسية في **فنلندا** لإنشاء نظام رقابة جماعية خاص بها. ففي يناير/كانون الثاني 2015 اقترح الفريق العامل في وزارة الدفاع تقديم قانون جديد يمنح الحكومة سلطات واسعة للرقابة على الاتصالات، ومنها اعتراض كوابل الانترنت التي تعبر حدودها وربطها بقوات الأمن والشرطة والدفاع.

شركات التكنولوجيا الأمريكية ضد الرقابة الجماعية

"لن يستخدم الناس التكنولوجيا التي لا يثقون بها. فالحكومات عرَّضت هذه الثقة للخطر، وعلى الحكومات أن تساعد على استعادة الثقة."

براد سميث، المستشار العام ونائب الرئيس التنفيذي، الشؤون القانونية والشركات، مايكروسوفت.

كانت شركات ميكروسوفت وأبل وغوغل وفيس بوك وياهو مدرجة في قائمة مؤلفة من تسع شركات تكنولوجية أمريكية تورطت في الموجة الأولى من تسريبات سنودن.[67] وقد أرسلت التسريبات التي كشفت عن أن وكالة الأمن الوطني دخلت إلى بيانات مستخدميها، بناء على أوامر سرية من المحكمة من خلال برنامج "بريزم"، موجات صادمة لجسم هذه الصناعة. وبالإضافة إلى التعاون مع طلبات وكالة الأمن الوطني، فإن تسريبات أخرى أظهرت وجود برامج سرية سمحت للوكالة بالوصول إلى بيانات بعض زبائن الشركات. وأظهرت تسريبات سنودن أن وكالة الأمن الوطني كانت تتنصت سراً على بيانات لدى غوغل وياهو، وأنها مرَّت بين مراكز بيانات الشركتين – وهو أمر ادعتا بأنهما لم تكونا على علم به.[68] وأشارت وثائق مسرَّبة أخرى أن وكالة الأمن الوطني كانت تستطيع الوصول إلى الرسائل الإلكترونية المشفَّرة ومكالمات "السكايب"،[69] وأنها عملت على تطوير برامج تمكّنها من الوصول عن بُعد إلى البيانات الموجودة على الهواتف الذكية آي فون وأندروير وبلاكبري.[70]

وقد واجهت الشركات الأمريكية **نكسة استهلاكية لأن أخبار التسريبات أضعفت الثقة بها وشكَّلت خطراً على عوائدها** – ولاسيما بين الزبائن خارج الولايات المتحدة. ففي دراسة مسحية أُجريت على 300 شركة بريطانية وكندية ونشرتها PEER 1 في يناير/كانون الثاني 2014، أشارت 25% من الشركات المبحوثة إلى أنها نقلت البيانات إلى خارج الولايات المتحدة نتيجة للتسريبات المتعلقة بوكالة الأمن الوطني، وقالت 18% منها إنها "تريد أن تعرف بالضبط أين يتم حفظ بياناتها".[71] ودعا بعض الحكومات شركات الانترنت إلى الاحتفاظ ببياناتها على خوادم محلية وليس في الولايات المتحدة، وشجّعتها على استخدام الخدمات التي لا ترسل بيانات إلى الولايات المتحدة. فعلى سبيل المثال، صرَّح وزير الداخلية الألماني هانز بيتر فردريك بأن "مَن يخشى التنصت على اتصالاته بأية طريقة، يجب أن يستخدم خدمة لا تمر عبر الخوادم الأمريكية".[72] وبالمثل، فقد أصرَّ وزير الاقتصاد الرقمي الفرنسي على أنه بات من الضروري الآن "وضع مراكز البيانات والخوادم على الأراضي الفرنسية لضمان أمن البيانات."[73]

وفي محاولة لاستعادة الثقة في برامجها وخدماتها، **تحدثت شركات التكنولوجيا الأمريكية الكبرى علناً ضد برامج الرقابة الجماعية الأمريكية في السنتين الماضيتين**. ودعا عدد من الشركات الكبرى حكومة الولايات المتحدة إلى إصلاح القوانين التي تدعم جمع البيانات الجماعية والاحتفاظ بها، وكشف النقاب عن المزيد من المعلومات بشأن ممارسات الرقابة الجماعية.

"لقد هزت التسريبات المتعلقة بأنشطة الرقابة الحكومية ثقة مستخدمينا، وقد آن الأوان كي تعمل حكومة الولايات المتحدة من أجل استعادة ثقة المواطنين في سائر أنحاء العالم".
ماريسا ماير، المدير التنفيذي، ياهو.[74]

وفي الأسابيع التي تلتْ التسريبات، **مارس بعض الشركات ضغوطاً على حكومة الولايات المتحدة من أجل زيادة الشفافية بشأن طلباتها بموجب قانون مراقبة المعلومات الاستخبارية الأجنبية (فيزا)**، وهو الآلية التي تستخدمها وكالة الأمن الوطني لجمع البيانات حول مستخدمي الانترنت الأجانب، وبحلول نهاية يونيو/حزيران 2013 قدمت ميكروسوفت وغوغل دعوى قانونية في الولايات المتحدة للسماح لهما بالكشف عن عدد المرات التي صدرت فيها أوامر للشركتين بالإفصاح عن البيانات بموجب قانون "فيزا".[75] وفي فبراير/شباط 2014 سمحت حكومة الولايات المتحدة، للمرة الأولى، لشركات ميكروسوفت وغوغل وفيس بوك وياهو بالإفصاح عن معلومات بشأن حجم البيانات التي كانت ملزمة قانونياً بتقديمها إلى وكالة الأمن الوطني.[76] وقالت الشركات إنها لم تتمكن من الإفصاح عن أعداد وأنواع الطلبات التي تلقتها بالضبط.[77]

وفي ديسمبر/كانون الأول 2013 أطلقت ثماني شركات – وهي غوغل وميكروسوفت وفيس بوك وتويتر وياهو و AOL، ولينكد إن وأبل، **الائتلاف العالمي لإصلاح الرقابة الحكومية**، الذي دعا حكومات العالم إلى التصدي للممارسات والقوانين التي تنظم الرقابة الحكومية على الأفراد والوصول إلى معلوماتهم".[78] ونشرَ الائتلاف الذي انضمَّت إليه شركتان أخريان، وهما "دروب بوكس" و"إيفرنوت"، ليصل إلى 10 شركات، رسالة مفتوحة موجَّهة إلى مجلس الشيوخ في الولايات المتحدة في نوفمبر/تشرين الثاني 2014، حثَّه فيها على إقرار "قانون الحرية". كما دعا الائتلاف إلى إجراء اصلاحات، منها: "منع وصول الحكومة إلى البيانات من دون اتِّباع إجراءات قانونية سليمة؛ والتأكد من عدم الطلب من المزوِّدين إنشاء بنية تحتية داخل حدود البلد؛ وتعزيز التدفق الحر للبيانات عبر الحدود؛ وتجنب نشوب نزاعات بين الدول من خلال وضع أُطر قوية ومبدئية وشفافة تنظم الطلبات القانونية للبيانات في الولايات القضائية".[79]

في مارس/آذار 2015 شارك الائتلاف، مع عدد من شركات التقانة الأخرى ومنظمات المدافعين عن الخصوصية وحقوق الإنسان، في إرسال رسالة مفتوحة موجَّهة إلى الرئيس أوباما ومدير الاستخبارات الوطنية جيمس كلابر، ومدير وكالة الأمن الوطني الأدميرال مايكل روجرز، من بين آخرين، دعوْهم فيها إلى وضع حد بشكل واضح وقوي وفعال لممارسات جمع المعلومات الجماعية بموجب "قانون الوطنية في الولايات المتحدة"، وهو القانون الذي يسمح بجمع تحليلات البيانات الجماعية من قبل وكالة الأمن الوطني.[80]

واتخذت شركات تقانة أخرى مثل "سيسكو"، التي تنتج معدات الفتح والإغلاق الرئيسية، تدابير أكثر راديكالية لتفادي قيام وكالة الأمن الوطني بالتنصت على معداتها. وقد وضعت الشركة سياسة جديدة نتيجة لتسريبات سنودن، حيث أنها تقدم لزبائنها الحساسين خيار شحن المعدات إلى عناوين زائفة، في محاولة لإحباط ما تقوم به وكالة الأمن الوطني.[81]

وبالإضافة إلى الدعوة إلى إجراء إصلاحات قانونية في الولايات المتحدة، عمل بعض الشركات على **زيادة تقنيات الأمن والتشفير التلقائية الذي توفره لمستخدمي برامجها وخدماتها**. وكانت شركة أبل الشركة الأولى تقوم بالتشفير بتشغيل القرص الكامل على نظام تشغيل الهاتف الخليوي عندما أطلقت هاتفها الجديد iOS 8 في سبتمبر/أيلول 2014.[82] وهذا يعني أن جميع البيانات على هواتف آي فون التي تحتوي على iOS 8 – أي الصور والرسائل الإلكترونية والصلات وتاريخ المكالمات – تكون مشفَّرة تلقائياً، ولا يمكن الدخول عليها بدون إدخال كلمة المرور الصحيحة. كما تستخدم الشركة التشفير المعروف باسم end-to-end من المرسل إلى المتلقي مباشرة لحماية خدمة الرسائل النصية والمكالمات بالفيديو، "آي ميسيج وفيس تايم"؛ وتقول شركة أبل إنها "لن يكون بمقدورها الالتزام بأوامر التنصت حتى لو أردنا ذلك".[83] وقد حذت غوغل حذوها بتوفير تشفير القرص الكامل في الأجهزة الجديدة المحملة بنظام التشغيل 5.0 Lollipop، مع أن عدداً قليلاً من مزودي سماعة أندرويد قد اعتمدوا ذلك النظام.

كما احتلت شركة "واتس آب" العناوين الرئيسية في وسائل الإعلام باستخدام مفتاح التشفير "end-to-end" في تطبيقات الرسائل السريعة، واعتمدت بروتوكول التشفير لتطبيق المصدر المفتوح الذي يسمى "تيكست سيكيور"الذي تم تطويره لحماية خصوصية المستخدمين. إن الخطوات التي اتخذتها شركات "أبل وغوغل وواتس آب" لزيادة التشفير منذ تسريبات سنودن تمثل علامة على أن ضغط المستهلكين يدفع هذه الشركات باتجاه توفير خصوصية أكبر ومعايير أمنية أشد.

إن هذه التطورات توفر حماية أكبر لحقوق المستخدمين في الخصوصية. بيد أن ثمة حكومات أعربت عن بواعث قلقها لأن التشفير الأقوى سيمنع الوكالات المكلفة بتنفيذ القوانين ووكالات الاستخبارات من الوصول إلى الاتصالات، وهددت بإرغام الشركات على إدخال أبواب خلفية كي تستطيع الوكالات الحكومية الوصول عبرها إلى البيانات.

وقد انتقد موظفون مكلفون بتنفيذ القوانين، ومن بينهم وزير العدل الأمريكي إريك هولدار ومدير مكتب التحقيقات الفدرالي جيمس كومي، شركة أبل وادَّعوا أن معايير التشفير الجديدة التي اعتمدتها الشركة ستمنعهم من الوصول إلى البيانات الموجودة على هواتف iphone لأغراض تنفيذ القوانين.[84] وفي يناير/كانون الثاني 2015، قال رئيس الوزراء البريطاني ديفيد كاميرون إنه إذا فاز حزبه في انتخابات عام 2015 (وقد فاز) فإن الحكومة الجديدة ستقدم مشروع قانون يمنح أجهزة الأمن سلطة قراءة جميع الرسائل التي تُرسل عبر الانترنت.[85] وقال:

"في حالات الخطورة القصوى كان من الممكن قراءة رسالة شخص ما أو الاستماع إلى مكالمته، أو التنصت على اتصالات هاتفه الخليوي... ويبقى السؤال: هل سنسمح لوسيلة اتصالات لا يمكن معها القيام بذلك بكل بساطة؟
وجوابي على السؤال هو: لا، يجب ألا نسمح بذلك".
ديفيد كاميرون، رئيس الوزراء البريطاني، يناير/كانون الثاني 2015.

بيد أن الهجمات الحكومية على التشفير لا تصمد أمام التدقيق. فعلى مدى سنوات، ما انفكَّ مكتب التحقيقات الفدرالي يوصي المواطنين باستخدام التشفير في هواتفهم كنوع من الحماية من الجرائم.[86] ويفيد الرأي الغالب بين خبراء التكنولوجيا

بأن من المستحيل وضع أبواب خلفية "للخيِّرين". ورداً على انتقادات مكتب التحقيقات الفدرالي لشركة أبل، كتب بروس شنير، وهو أحد أبرز المسؤولين في مجال التشفير وأمن الحاسوب في العالم، يقول:

"لا يمكنك بناء باب خلفي لا يمرُّ منها سوى الأشخاص الأخيار. فالتشفير يحمي من المجرمين الإلكترونيين والمنافسين الصناعيين ومن الشرطة السرية الصينية ومكتب التحقيقات الفدرالي. فإما أن تتعرض للتنصت من قبل أي منهم، أو أن تكون آمناً من التنصت عليك من قبلهم جميعاً."

بروس شنير [87]

ورداً على تصريح ديفيد كاميرون، قال كوري دكتورو، الكاتب في مجال التكنولوجيا:
"إذا وضعتْ تطبيقات واتس أب أو غوغل مثلبة متعمدة فيها، فإن الجواسيس الأجانب والمجرمين وأفراد الشرطة الفاسدين... سوف يكتشفون نقطة الضعف هذه في نهاية المطاف. وسيتمكن هؤلاء – وليس أجهزة الأمن فحسب – من استخدامها للتنصت على جميع اتصالاتنا. وهذا يشمل أشياء من قبيل صور أطفالك في الحمام التي ترسلها إلى والديك، وأسرار التجارة التي ترسلها إلى شركائك في العمل."[88]

إن شركات التكنولوجيا ينبغي أن تلعب دوراً مهماً جداً في حماية الحق في الخصوصية. وباعتماد معايير تشفير أقوى، تستطيع أن تكفل حماية اتصالات ملايين مستخدِمي الانترنت من الرقابة المتطفلة والهجمات الإجرامية. وإن الشركات التي تفشل في ذلك، لا تخذل مستخدميها وتفقدهم الثقة بها فحسب، وإنما ربما تتخلى عن مسؤوليتها تجاه احترام حقهم في الخصوصية. وثمة خطوات أخرى تستطيع الشركات ويجب أن تتخذها لضمان إحاطة زبائنها علماً بالمخاطر التي تتهدد حقوقهم الإنسانية على نحو أفضل. فعلى سبيل المثال، يتعين عليها أن تبلغهم بالشروط القانونية لتسليم بيانات المستخدمين إلى الحكومات، بشفافية ووضوح، في كل ولاية قضائية تعمل في ظلها.

"إذا كانت [أجهزة الأمن] صادقة حقاً، فإنها تعلم أن منع التشفير من شأنه أن يعاقب "الأخيار"، لا أن يمنع "الأشرار". وليس ثمة مقايضة. إن ذلك لا ينجح أساساً. لا بد من إيجاد حلول أخرى."

تيم كوك، المدير التنفيذي لشركة أبل، 27 فبراير/شباط 2014.

التقدم إلى الأمام

بعد مرور عامين على تسريبات سنودن، لا تزال أجهزة الرقابة الجماعية الضخمة التي تشغّلها وكالات الاستخبارات في الولايات المتحدة والمملكة المتحدة على حالها، ولا يلوح في الأفق مؤشرات على أنها تعتزم وقف استخدام – وتوسيع – قدراتها.

وعلى الرغم من المعلومات التي سُربت إلى الرأي العام، فإن برامج الرقابة الجماعية البريطانية والأمريكية لا تزال محاطة بالسرية. ولا شيء يوضح هذا الأمر أفضل من سياسة الحكومة البريطانية المعروفة باسم "لا نؤكد ولا ننفي". وقد أدت سياسة عدم التأكيد وعدم النفي أولئك الذين رفعوا دعاوى قانونية ضد برامج الرقابة الجماعية البريطانية أمام خيار واحد

فقط، وهو تقديم محاججات قانونية حول سيناريوهات افتراضية. وهذا يعني أن البرامج الفعلية، من قبيل "تيمبورا"، التي يقوم وجودها بشكل واضح على وثائق كشف عنها النقاب إدوارد سنودن، ظلت محصنة من أي نوع من التدقيق الحقيقي.

وعلى الرغم من الإدانة الواسعة النطاق لممارسات الرقابة الجماعية من قبل الولايات المتحدة والمملكة المتحدة بصفتها تشكل انتهاكاً لحقوق الإنسان، وقرارات الحكم التي أصدرتها المحاكم في كلا البلدين، والتي قضت بأن بعض تلك الممارسات غير قانوني، فإنه لم يخضع أحد للمساءلة على السماح باستخدام تلك البرامج المتطفلة على ما يبدو.

إن الرسالة التي تبعث بها الولايات المتحدة والمملكة المتحدة، إلى جانب شريكاتهما الوثيقة الصلة، أستراليا وكندا ونيوزيلندا، هي رسالة واضحة مفادها: أن هذه الحكومات لن تتخلى بسهولة عن برامج الرقابة الجماعية. وبالإضافة إلى ذلك، فقد شهدنا في السنتين الماضيتين منذ ظهور تسريبات سنودن عدداً متنامياً من البلدان، كمصر[89] وفرنسا [90] وباكستان،[91] التي تسعى إلى زيادة قدراتها في مجال مراقبة الاتصالات.

تتزايد الأخطار التي تتهدد الخصوصية على الانترنت، وتتزايد معها الأخطار على حرية التعبير، ويتنامى نضال الصحفيين الذين يقومون بفضح برامج الرقابة، ومنظمات المجتمع المدني التي تتحدى الرقابة الجماعية، والشركات التي عززت حماية الخصوصية في منتجاتها. أما الأمر الأكثر أهمية من ذلك، منذ تسريبات سنودن، فهو أن مئات الملايين من مستخدمي الانترنت اتخذوا خطوات لحماية خصوصيتهم على الانترنت.[92]

إن هذه الأنشطة المتنامية هي التي تواجه خطر الرقابة المتفشية، حيث تتجسس الحكومات على كل شيء وكل شخص في كل الأوقات. وإن التقدم التكنولوجي يعني أن تقانة الرقابة ستصبح أقل ثمناً وأشد قوة. وإن العديد من القدرات المتوفرة حالياً لدى وكالة الأمن الوطني وقيادة الاتصالات الحكومية وحدهما ستصبح شائعة في غضون سنوات قليلة. إن حماية الخصوصية، وبالتالي حرية التعبير، في هذا العصر الرقمي تقتضي التحرك على جبهات عدة: الاستخدام الواسع النطاق وغير المقيَّد للتشفير القوي والأدوات المجهولة الهوية؛ والإصلاحات القانونية والسياسية الوطنية واحترام المعايير الدولية؛ وحماية كاشفي التجاوزات وكشف النقاب عن المعلومات التي تهمُّ المصلحة العامة، من قبيل الأدلة على وقوع انتهاكات حقوق الإنسان.

إن خطة النقاط السبع التالية تعتبر نداء للتحرك موجهاً إلى منظمات المجتمع المدني والمتخصصين في التكنولوجيا والخبراء والشركات والحكومات التي تريد المحافظة على المثُل العليا التي بُني عليها الانترنت: وهي الحرية والانفتاح وإمكانية الوصول إليها. ونحن نؤمن أن هذه الخطوات تُعتبر أساسية لضمان حماية حقوق الإنسان في عصرنا الرقمي.

الإصلاحات القانونية والسياسية

1. ينبغي إصلاح القوانين الوطنية لضمان اتساقها مع القانون الدولي لحقوق الإنسان، بما في ذلك عن طريق عدم السماح بالرقابة الجماعية العشوائية. أما المبادئ الرئيسية التي ينبغي احترامها؛ فهي:

أ) ضمان عدم مراقبة الاتصالات إلا عندما تكون مستهدفة، ومستندة إلى أدلة كافية على ارتكاب أفعال خاطئة، ومرخصة من قبل سلطة مستقلة وصارمة كالقضاء؛

ب) ضمان وجود إشراف برلماني وقضائي شفاف ومستقل على سلطات الرقابة؛

ج) إتاحة القواعد والسياسات المتعلقة بالرقابة للجمهور العام، بما في ذلك تبادل الحكومات للمعلومات مع دول أخرى؛

د) ضمان تطبيق أشكال حماية الخصوصية على المواطنين وغير المواطنين، وعلى الذين يعيشون داخل أراضي الدولة والذين يعيشون خارج أراضيها على قدم المساواة؛

هـ) ينبغي تنظيم وتنفيذ عمليات تبادل المعلومات الاستخبارية بطريقة تتقيد بالتزامات الدول بحقوق الإنسان؛

2. يجب ألا تجعل الحكومات تقنيات التشفير وعدم الكشف عن الهوية، أو استخدامها، أمراً غير قانوني؛

3. ينبغي توفير حماية قانونية قوية لكاشفي التجاوزات، بمن فيهم أولئك الذين يعملون في مجال قضايا الأمن القومي، من أي شكل من أشكال الانتقام، ومنها الملاحقة القضائية، بسبب كشفهم عن معلومات تَهمُّ المصلحة العامة، من قبيل انتهاكات حقوق الإنسان.[93]

الدأب الواجب للشركات

<u>تماشياً مع مسؤولية الشركات نحو احترام حقوق الإنسان:</u>

4. يتعين على الشركات التي تملك و/أو تشغِّل البنية التحتية للاتصالات السلكية واللاسلكية أو الانترنت، ومنها كوابل الاتصالات البحرية، وشركات الانترنت، أن تكفل السماح بالوصول إلى البيانات المتعلقة بحقوق الإنسان، بما في ذلك عن طريق اتخاذ إجراءات قانونية للطعن في طلبات الحكومات التي تسعى إلى الوصول إلى الاتصالات بالجملة؛

5. يجب أن تقود شركات الانترنت والاتصالات الكبرى الطريق إلى استخدام التشفير القوي وغيره من تقنيات الخصوصية، بما في ذلك من خلال استخدام تشفير التوصيل المباشر end-to-end تلقائياً، حيثما يكون ذلك ممكناً؛

6. يتعين على مزوِّدي خدمات الانترنت وشركات الاتصالات وشركات الانترنت إبلاغ المستخدمين بوضوح بالشروط القانونية التي ينبغي أن تفي بها، ولاسيما فيما يتعلق بتسليم معلومات أو محتويات خاصة بالمستخدمين.

المعايير الدولية

7. استكشاف وتطوير المزيد من الوسائل والتدابير الضرورية لضمان تنفيذ المعايير الدولية لحقوق الإنسان التي تنطبق على مراقبة الاتصالات على نحو أفضل، والبناء على الجهود التي بُذلت بهدف تحديد العناصر ذات الصلة التي بدأت في السنتين الماضيتين، ومنها تقرير المقرر الخاص للأمم المتحدة المعني بحرية التعبير،[94] والمفوض السامي للأمم المتحدة لحقوق الإنسان والمقرر الخاص المعني بتعزيز وحماية حقوق الإنسان والحريات الأساسية في سياق مكافحة الارهاب،[95] بالإضافة إلى مبادرات المجتمع المدني، من قبيل مبدأيْ الضرورة والتناسب.[96]

الهوامش

1. توحيد وتعضيد أمريكا من خلال الإيفاء بالحقوق وضمان فرض نظام فعال على قانون المراقبة لعام 2015 (قانون الحرية لعام 2015)، **H.R.— 114th Congress (2015-2016)**

2. للمزيد من المعلومات، أنظر منظمة الخصوصية الدولية، العيون الخمس، على الرابط: https://www.privacyinternational.org/?q=node/51

3. أنظر "ذي واشنطن بوست"، وكالة الأمن الوطني، شريحة تُظهر كوابل المراقبة البحرية، 10 يوليو/تموز 2013، أنظر الرابط: http://www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html؛ وصحيفة "ذي غارديان"، *قيادة الاتصالات الحكومية تعترض كوابل الألياف البصرية للوصول بشكل سري إلى اتصالات العالم*" ، أنظر الرابط: http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

4. العصب البصري: التنصت على ملايين صور الكاميرا على شبكة الانترنت على موقع ياهو من قبل قيادة الاتصالات الحكومية، ذي غارديان، 28 فبراير/شباط 2014، انظر: http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo

5. كندا تلقي شبكة جرافة عالمية لمراقبة تنزيل الملفات، 18 يناير/كانون الثاني 2015، أنظر الرابط: https://firstlook.org/theintercept/2015/01/28/canada-cse-levitation-mass-surveillance

6. مؤسسة أمن الاتصالات الكندية تراقب ملايين الرسائل الإلكترونية الكندية الموجهة إلى الحكومة، سي بي سي نيوز، 25 فبراير/شباط 2015، أنظر الرابط: http://www.cbc.ca/news/cse-monitors-millions-of-canadian-emails-to-government-1.2969687

7. نيوزيلندا تتجسس على جيرانها سراً، الرقابة العالمية "للعيون الخمس"، 3 أبريل/نيسان 2015، أنظر الرابط: https://firstlook.org/theintercept/2015/03/04/new-zealand-gcsb-surveillance-waihopai-xkeyscore

8. شرائح برنامج "بريزم" الذي تشغِّله وكالة الأمن الوطني، ذي غارديان، 1 نوفمبر/تشرين الثاني 2013، أنظر الرابط: http://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document

9. أسئلة وأجوبة: خطة "بريزم" للرقابة على الانترنت التي تقوم بها وكالة الأمن الوطني، بي بي سي، 1 يوليو/تموز 2013، أنظر: http://www.bbc.co.uk/news/technology-23051248

10. *وكالة الأمن الوطني تخترق الروابط إلى مراكز البيانات في ياهو وغوغل في سائر العالم*، هكذا تقول وثائق سنودن، واشنطن بوست، 30 أكتوبر/تشرين الأول 2013، أنظر الرابط: http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html

11. عملية الاشتراكي: القصة الداخلية عن قرصنة جواسيس بريطانيين لأكبر شركة اتصالات بلجيكية، "ذي انترسيبت"، 13 ديسمبر/كانون الأول 2014، أنظر الرابط: https://firstlook.org/theintercept/2014/12/13/belgacom-hack-gchq-inside-story

12. وكالة الأمن الوطني تتعقَّب مواقع الهواتف الخليوية: هذا ما تُظهره وثائق سنودن، واشنطن بوست، 4 ديسمبر/كانون الأول 2013، أنظر: http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html

13. برنامج المراقبة الذي تديره وكالة الأمن الوطني "يذهب إلى الماضي" بهدف استعادة المكالمات الهاتفية وإعادة تشغيلها، واشنطن بوست، 18 مارس/آذار 2014، أنظر الرابط:

http://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.htm

14. سنودن: وكالات التجسس الأمريكية مارست ضغوطاً على دول الاتحاد الأوروبي لحملها على تخفيف قوانين الخصوصية، ذي فايننشال تايمز، 7 مارس/آذار 2014، انظر الرابط:

http://www.ft.com/cms/s/0/9f45bcb2-a616-11e3-8a2a-00144feab7de.html#axzz3a7iVHH6t

15. المصدر نفسه

16. قيادة الاتصالات الحكومية البريطانية ووكالات التجسس الأوروبية عملت معاً في مجال الرقابة الجماعية، 1 نوفمبر/تشرين الثاني 2013. أنظر الرابط:

http://www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden

17. كيف يقوم الشركاء السريون بتوسيع نطاق شبكة الرقابة التابعة لوكالة الأمن الوطني، "ذي انترسيبت"، 19 يونيو/حزيران 2014، أنظر الرابط:

https://firstlook.org/theintercept/2014/06/18/nsa-surveillance-secret-cable-partners-revealed-rampart-a

18. المصدر نفسه

19. "بي أن دي" تخزّن 220 مليون مكالمة هاتفية كل يوم، زيت أون لاين، 2 فبراير/شباط 2015، أنظر:

http://www.zeit.de/digital/datenschutz/2015-02/bnd-nsa-mass-surveillance

20. تسريبات: كيف تنتهك وكالات التجسس الأمريكية والبريطانية خصوصية وأمن الانترنت، ذي غارديان، 6 سبتمبر/أيلول 2013، أنظر:

http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

21. وكالة الأمن الوطني قادرة على إبطال ضمانات الخصوصية على الشبكة العنكبوتية، ذي نيويورك تايمز، 5 سبتمبر/أيلول 2013، انظر الرابط:

http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?hp&_r=0

22. تسريبات: كيف تنتهك وكالات التجسس الأمريكية والبريطانية خصوصية وأمن الانترنت، ذي غارديان، 6 سبتمبر/أيلول 2013، أنظر الرابط:

http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

23. حصري: وكالة الأمن الوطني تدفع 100 مليون جنيه استرليني كتمويل سري لقيادة الاتصالات الحكومية البريطانية، ذي غارديان، 1 أغسطس/آب 2013، أنظر الرابط:

http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden

24. ينبغي تحديد المصدر

25. كيف تخطط وكالة الأمن الوطني لإصابة ملايين الحواسيب بالبرمجيات الخبيثة، "ذي انترسيبت"، 3 ديسمبر/كانون الأول 2014، أنظر:

https://firstlook.org/theintercept/2014/03/12/nsa-plans-infect-millions-computers-malware

26. الكشف عن صندوق أدوات الحرب الإلكترونية لمؤسسة أمن الاتصالات، سي بي سي نيوز، 2 أبريل/نيسان 2015، انظر:

http://www.cbc.ca/news/canada/communication-security-establishment-s-cyberwarfare-toolbox-revealed-1.3002978

27. ispy كيف تدخل وكالة الأمن الوطني إلى بيانات الهواتف الخليوية، دير شبيغل، 9 سبتمبر/أيلول 2013، أنظر:

http://www.spiegel.de/international/world/how-the-nsa-spies-on-smartphones-including-the-blackberry-a-921161.html

28. غلين غرينوالر، لا مكانا للاختباء فيه، 2014، ص. 105.

29. داخل TAO: وثائق تكشف النقاب عن وحدة القرصنة الأولى في وكالة الأمن الوطني، دير شبيغل، 29 ديسمبر/كانون الأول 2013، أنظر:

http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969-3.htm

30. عملية السطو الكبرى على شريحة هوية المشترك SIM: كيف سرق الجواسيس مفاتيح قلعة التشفير، "ذي انترسيبت"، 19 فبراير/شباط 2015، أنظر الرابط:
https://firstlook.org/theintercept/2015/02/19/great-sim-heist

31. الحرية والأمن في عالم متغير: تقرير وتوصيات فريق الرئيس الاستشاري المعني بتقانة المعلومات الاستخبارية والاتصالات، 12 ديسمبر/كانون الأول 2013، التوصية رقم 4، ص 25، أنظر الرابط:
https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

32. قرار الجمعية العامة للأمم المتحدة رقم 68/167: الحق في الخصوصية في العصر الرقمي، 18 ديسمبر/كانون الأول 2013، أنظر الرابط:
http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167

33. مجلس مراقبة الخصوصية والحريات المدنية، تقرير حول التسجيلات الهاتفية أُعد بموجب الفصل 215 من قانون الوطنية في الولايات المتحدة وحول عمليات محكمة مراقبة المعلومات الاستخبارية الأجنبية، أنظر الرابط:
https://www.documentcloud.org/documents/1008937-final-report-1-23-14.html

34. أنظر: http://www.europarl.europa.eu/committees/en/libe/subject-files.html?id=20130923CDT71796

35. أنظر: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

36. أنظر: https://firstlook.org/theintercept/document/2014/10/15/un-report-human-rights-terrorism

37. أنظر: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/69/16

38. أنظر:
https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2734552&SecMode=1&DocId=2262340&Usage=2

39. أنظر: http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21692&lang=en

40. أنظر: https://www.privacyinternational.org/sites/default/files/SR%20resolution.pdf

41. أنظر: https://www.privacyinternational.org/sites/default/files/SR%20resolution.pdf

42. للاطلاع على مزيد من المعلومات، أنظر: https://www.privacyinternational.org/?q=node/51

43. يمكن الاطلاع على الحكم عبر الرابط: http://www.ipt-uk.com/docs/Liberty_Ors_Judgment_6Feb15.pdf؛ وعلى الأمر عبر الرابط: http://www.ipt-uk.com/docs/Liberty-Order6Feb15.pdf

44. أنظر الرابط: https://www.privacynotprism.org.uk، ومكتب الصحافة الاستقصائية، ملخص طلب المكتب المقدم إلى المحكمة الأوروبية لحقوق الإنسان، 14 سبتمبر/أيلول 2014، انظر:
https://www.thebureauinvestigates.com/2014/09/14/a-summary-of-the-bureaus-application-to-the-european-court-of-human-rights

45. للاطلاع على مزيد من المعلومات، أنظر الرابط: https://www.privacyinternational.org/?q=node/459

46. للاطلاع على مزيد من المعلومات، أنظر الرابط: https://www.privacyinternational.org/?q=node/81

47. محكمة الاستئناف، الدائرة الثانية، قضية "ألكو" ضد كلابر، رقم 42-14، بتاريخ 7 مايو/أيار 2015، أنظر:
http://pdfserver.amlaw.com/nlj/NSA_ca2_20150507.pdf

48. المصدر نفسه

49. المصدر نفسه

50. رابطة الحريات المدنية في كولومبيا البريطانية، الرابطة تقاضي الحكومة الكندية لوقف التجسس غير القانوني، أنظر الرابط: https://bccla.org/stop-illegal-spying/protect-our-privacy-case-details/ :

51. لمزيد من المعلومات، أنظر الرابط: http://www.igis.govt.nz/announcements/

52. لمزيد من المعلومات، أنظر الرابط:
https://www.privacyfirst.eu/actions/litigation/item/616-district-court-of-the-hague-wide-off-the-mark-in-citizens-v-plasterk-case.html

53. قيادة الاتصالات الحكومية ووكالة الأمن الوطني استهدفتا جمعيات خيرية وألمان وعضو في البرلمان الإسرائيلي ومسؤول في الاتحاد الأوروبي، أنظر الرابط:
http://www.theguardian.com/uk-news/2013/dec/20/gchq-targeted-aid-agencies-german-government-eu-commissioner

54. أنظر الرابط: http://doctorsoftheworld.org.uk/pages/what-we-do

55. ليه دينز، أطباء العالم: كيف اكتشفنا أن قيادة الاتصالات الحكومية كانت تتجسس علينا، 20 أبريل/نيسان 2015، أنظر الرابط:
https://www.opendemocracy.net/digitaliberties/leigh-daynes/doctors-of-world-how-we-discovered-gchq-was-spying-on-our-operations

56. خواكين ألمونيا، الصلاحيات، أنظر الرابط:
http://ec.europa.eu/archives/commission_2010-2014/almunia/about/mandate/index_en.htm

57. قيادة الاتصالات الحكومية ووكالة الأمن الوطني استهدفتا جمعيات خيرية وألمان وعضو برلمان إسرائيلي ومسؤول في الاتحاد الأوروبي، أنظر:
http://www.theguardian.com/uk-news/2013/dec/20/gchq-targeted-aid-agencies-german-government-eu-commissioner

58. أنظر الرابط: http://www.unicef.org/about/who/index_introduction.html

59. حكومة الولايات المتحدة صنَّفت صحفياً بارزاً في الجزيرة بأنه عضو في تنظيم القاعدة، ذي انترسيبت، 8 مايو/أيار 2015، أنظر:
https://firstlook.org/theintercept/2015/05/08/u-s-government-designated-prominent-al-jazeera-journalist-al-qaeda-member-put-watch-list

60. مقابلة مع الزعيم الأمريكي المسلم، الذي تجسس عليه مكتب التحقيقات الفدرالي ووكالة الأمن الوطني، 9 يوليو/تموز 2014، أنظر:
https://firstlook.org/theintercept/2015/05/08/u-s-government-designated-prominent-al-jazeera-journalist-al-qaeda-member-put-watch-list

61. منظمة الحرية، منظمة الخصوصية الدولية، مجموعة الحقوق المفتوحة، منظمة مراقبة الشقيق الأكبر، والمادة 19، والتقرير الموجز لرابطة القلم PEN الإنجليزية حول مشروع قانون الاحتفاظ بالبيانات وسلطات التحقيق، على الرابط:
https://www.libertyhumanrights.org.uk/sites/default/files/Briefing%20on%20the%20Data%20Retention%20and%20Investigatory%20Powers%20Bill.pdf

62. التوجيه الرئاسي الخاص بالسياسات رقم 28، أنشطة الإشارات الدفاعية الاستخبارية، 17 يناير/كانون الثاني 2014، أنظر الرابط:
https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities

63. توحيد وتعضيد أمريكا من خلال الإيفاء بالحقوق وضمان فرض نظام فعال في قانون المراقبة لعام 2015 (قانون الحرية لعام 2015)، H.R.— 114th Congress (2015-2016)

64. بيان مشترك من المادة 19، منظمة مراقبة حقوق الإنسان، ومنظمة الخصوصية الدولية، ومؤسسة الحقوق الرقمية؛ وغيرها في قانون منع الجرائم الإلكترونية لعام 2015، باكستان، أنظر الرابط:
https://www.privacyinternational.org/sites/default/files/Prevention-of-Electronic-Crimes-Bill-International-Joint-Statement_2.pdf

65. قانون تقييم أجهزة المخابرات والأمن لعام 2002. نحو إيجاد توازن بين السلطات والضمانات، نُشر في 2 ديسمبر/كانون الأول 2013. من الصفحة 171 فصاعداً (التوصية 5.8).

66. موقف الحكومة بشأن مراقبة قانون أجهزة الأمن والمخابرات لعام 2002، رقم 41-33820، بتاريخ 21 نوفمبر/تشرين الثاني 2014، أنظر الرابط:https://zoek.officielebekendmakingen.nl/kst-33820-4.html

67. ذي واشنطن بوست، الولايات المتحدة، تمحيص البيانات الاستخبارية الأمريكية والبريطانية من تسع شركات انترنت أمريكية ضمن برنامج سري واسع، 7 يونيو/حزيران 2013، أنظر الرابط:

http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

68. ذي غارديان، التقارير التي تفيد بأن وكالة الأمن الوطني تتنصت على بيانات غوغل وياهو تثير غضب عمالقة التكنولوجيا، 31 أكتوبر/تشرين الأول 2013، أنظر الرابط:

http://www.theguardian.com/technology/2013/oct/30/google-reports-nsa-secretly-intercepts-data-links

69. "ذي غارديان"، ميكروسوفت أتاحت لوكالة الأمن الوطني إمكانية الوصول إلى الرسائل المشفرة، 12 يوليو/تموز 2013، أنظر الرابط:

http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data

70. شبيغل أون لاين، ispy: كيف تصل وكالة الأمن الوطني إلى بيانات الهواتف الذكية، 9 سبتمبر/أيلول 2013، أنظر الرابط:

http://www.spiegel.de/international/world/how-the-nsa-spies-on-smartphones-including-the-blackberry-a-921161.html

71. معهد التكنولوجيا المفتوح، تكاليف الرقابة: أثر وكالة الأمن الوطني على الاقتصاد وحرية الانترنت والأمن الإلكتروني، يوليو/تموز 2014، أنظر الرابط:

http://www.newamerica.org/downloads/Surveilance_Costs_Final.pdf، ص 8

72. جونا فورس هيل، نحو محلية البيانات في مرحلة ما بعد سنودن: تحليل وتوصيات إلى صانعي السياسات وقادة الصناعة في الولايات المتحدة، 21 يوليو/تموز 2014، أنظر الرابط:

http://www.lawfareblog.com/wp-content/uploads/2014/07/Lawfare-Research-Paper-Series-Vol2No3.pdf، ص 6

73. المصدر نفسه.

74. "ذي واشنطن بوست"، الشركات التكنولوجية الكبرى تتحد من أجل الدعوة إلى وضع حدود جديدة للرقابة، 9 ديسمبر/كانون الأول 2013، أنظر الرابط:

http://www.washingtonpost.com/business/technology/major-tech-companies-unite-to-call-for-new-limits-on-surveillance/2013/12/08/530f0fd4-6051-11e3-bf45-61f69f54fc5f_story.html

75. "ذي غارديان"، ميكروسوفت تنضم إلى غوغل في المطالبة بالإفصاح عن طلبات "فيسا"، 28 يونيو/حزيران 2013، أنظر الرابط:

http://www.theguardian.com/technology/2013/jun/28/microsoft-google-fisa-united-states-government

76. "ذي غارديان"، ميكروسوفت وفيس بوك وغوغل وياهو تكشف النقاب عن طلبات الرقابة الأمريكية، 3 فبراير/شباط 2014، أنظر الرابط:

http://www.theguardian.com/world/2014/feb/03/microsoft-facebook-google-yahoo-fisa-surveillance-requests؛و"ذي غارديان"، شركات التكنولوجيا العملاقة تتوصل إلى صفقة مع البيت الأبيض بشأن الرقابة على بيانات الزبائن التي تمارسها وكالة الأمن الوطني، 27 يناير/كانون الثاني 2014، أنظر الرابط:

http://www.theguardian.com/world/2014/jan/27/tech-giants-white-house-deal-surveillance-customer-data

77. "ذي غارديان"، ميكروسوفت وفيس بوك وغوغل وياهو تكشف النقاب عن طلبات الرقابة الأمريكية، 3 فبراير/شباط 2014، على الرابط:
http://www.theguardian.com/world/2014/feb/03/microsoft-facebook-google-yahoo-fisa-surveillance-requests

78. أنظر الرابط: https://www.reformgovernmentsurveillance.com

79. أنظر الرابط: http://reformgs.tumblr.com/post/102821955852/open-letter-to-the-us-senate

80. أنظر الرابط:
https://static.newamerica.org/attachments/2579-nsa-coalition-letter/NSA_coalition_letter_032515_politico.pdf

81. سيسكو ترسل طروداً إلى منازل خالية لتجنب "محلات بيع القطع المسروقة" التابعة لوكالة الأمن الوطني، ذي ريجستر، 18 مارس/آذار 2015، انظر الرابط:
http://www.theregister.co.uk/2015/03/18/want_to_dodge_nsa_supply_chain_taps_ask_cisco_for_a_dead_drop/?mt=1426694168077

82. "آرس تكنيكا"، شركة أبل توسِّع نطاق تشفير البيانات بموجب I058، وتسلمه بلا معنى، 18 سبتمبر/أيلول 2014، أنظر الرابط:
http://arstechnica.com/apple/2014/09/apple-expands-data-encryption-under-ios-8-making-handover-to-cops-moot

83. أنظر الرابط: https://www.apple.com/uk/privacy/privacy-built-in

84. رويترز، وزير العدل الأمريكي ينتقد تشفير بيانات أبل وغوغل، 30 سبتمبر/أيلول 2014، أنظر الرابط:
http://www.reuters.com/article/2014/09/30/us-usa-smartphones-holder-idUSKCN0HP22P20140930

85. "ذي تلغراف"، ديفيد كاميرون يقول إن الجواسيس يجب أن يتمكنوا من مراقبة كافة الرسائل على الانترنت، 12 يناير/كانون الثاني 2015 أنظر الرابط:
http://www.telegraph.co.uk/technology/internet-security/11340621/Spies-should-be-able-to-monitor-all-online-messaging-says-David-Cameron.html

86. القذارة التكنولوجية، مكتب التحقيقات الفدرالي يشطب التوصية المتعلقة بتشفير هواتفكم بهدوء ... بينما يحذر مدير الوكالة من أن التشفير سيؤدي إلى ذرف الدموع، 26 مارس/آذار 2015، أنظر الرابط:
https://www.techdirt.com/articles/20150325/17430330432/fbi-quietly-removes-recommendation-to-encrypt-your-phone-as-fbi-director-warns-how-encryption-will-lead-to-tears.shtml

87. بروس شنير، تشفير آي فون وعودة حروب التشفير، 6 أكتوبر/تشرين الأول 2014، أنظر الرابط:
https://www.schneier.com/blog/archives/2014/10/iphone_encrypti_1.html

88. كوري دوكتورو، إن ما اقترحه ديفيد كاميرون للتو من شأنه أن يعرِّض كل بريطاني للخطر وأن يدمر صناعة تكنولوجيا المعلومات، أنظر الرابط:
http://boingboing.net/2015/01/13/what-david-cameron-just-propos.html

89. أنظر منظمة العفو الدولية: خطة الحكومة المصرية المتعلقة بفرض الرقابة الجماعية على وسائل التواصل الاجتماعي تعتبر هجوماً على خصوصية الانترنت وحرية التعبير، 4 يونيو/حزيران 2014، أنظر الرابط:
https://www.amnesty.org/en/articles/news/2014/06/egypt-s-attack-internet-privacy-tightens-noose-freedom-expression/؛

و"أنت تحت المراقبة!"، الرقابة الجماعية على الانترنت في مصر، مدى مصر، 29 سبتمبر/أيلول 2014. أنظر الرابط:
https://www.amnesty.org/en/articles/news/2014/06/egypt-s-attack-internet-privacy-tightens-noose-freedom-expression/

90. أنظر منظمة العفو الدولية: فرنسا: أوقفوا الاندفاع نحو دولة الرقابة، 4 مايو/أيار 2015، على الرابط:
https://www.amnesty.org/en/articles/news/2015/05/france-surveillance-state/؛ ومنظمة العفو الدولية: فرنسا:
France: les députés approuvent la surveillance de masse, 5 May 2015 ، بتاريخ 5 مايو/أيار 2015، على الرابط:
http://www.amnesty.fr/Nos-campagnes/Liberte-expression/Actualites/France-les-deputes-approuvent-la-surveillance-de-masse-15061

91. أنظر منظمة الخصوصية الدولية: المنظمات الدولية لحقوق الإنسان تشعر بالقلق العميق بشأن قانون منع الجرائم الإلكترونية لعام 2015، باكستان، 20 أبريل/نيسان 2015، أنظر الرابط:
https://www.privacyinternational.org/?q=node/566

92. بيل شنير، ما يربو على 700 مليون شخص يتخذون خطوات لتفادي الرقابة من قبل وكالة الأمن الوطني، 15 ديسمبر/كانون الأول 2014، أنظر الرابط:https://www.schneier.com/crypto-gram/archives/2014/1215.html#7

93. أنظر المبادئ العالمية للأمن القومي والحق في المعلومات (مبادئ تشواني)، أنظر الرابط:
http://www.opensocietyfoundations.org/publications/global-principles-national-security-and-freedom-information-tshwane-principles؛ وأنظر أيضاً: الجمعية البرلمانية لمجلس أوروبا، الأمن الوطني والحصول على المعلومات، القرار رقم 1954 (2013)، الذي رحَّب باعتماد مبادى تشواني، أنظر الرابط:
http://assembly.coe.int/nw/xml/XRef/X2H-Xref-ViewPDF.asp?FileID=20190&lang=en

94. مجلس حقوق الإنسان، تقرير المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير، فرانك لا روي، رقم الوثيقة: A/HRC/23/40، بتاريخ 17 أبريل/نيسان 2013، على الرابط:
http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

95. الجمعية العامة، تقرير المقرر الخاص المعني بتعزيز وحماية حقوق الإنسان والحريات الأساسية في سياق مكافحة الإرهاب، رقم الوثيقة: A/69/397 ,، بتاريخ 23 سبتمبر/أيلول 2014. أنظر الرابط:
http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N14/545/19/PDF/N1454519.pdf?OpenElement

96. المبادئ الدولية المتعلقة بتطبيق حقوق الإنسان في عمليات الرقابة على الاتصالات، مايو/أيار 2014، أنظر الرابط:
https://en.necessaryandproportionate.org/